Microsoft.SC-200J.v2026-08-13.q178

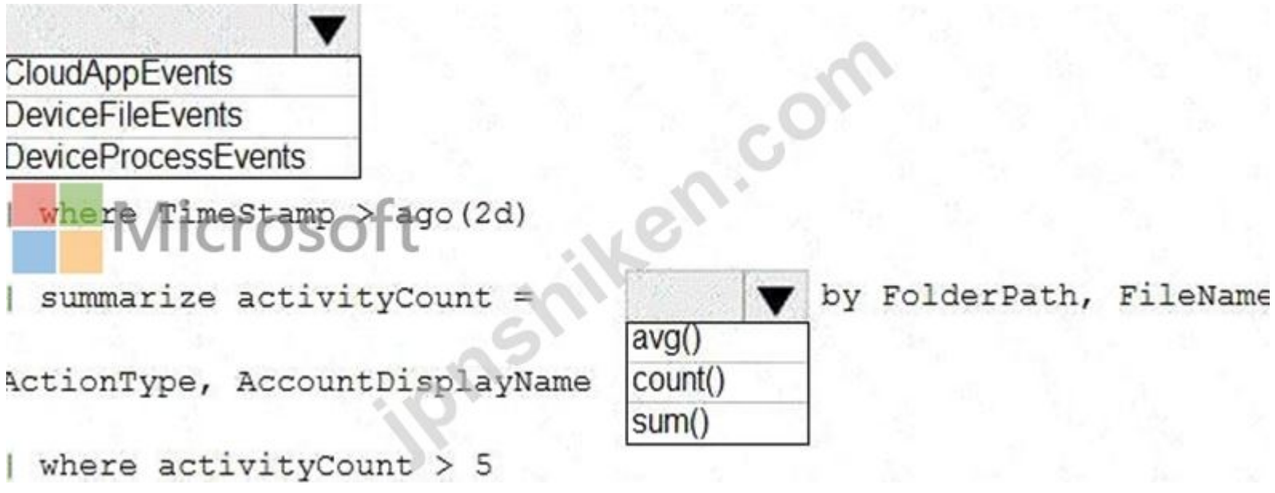
試験コード：	SC-200J
試験名称：	Microsoft Security Operations Analyst (SC-200日本語版)
認証ベンダー：	Microsoft
無料問題の数：	178
バージョン：	v2026-08-13
ページの閲覧量：	105
問題集の閲覧量：	2240

https://www.jpnshiken.com/shiken/Microsoft.SC-200J.v2026-08-13.q178.html

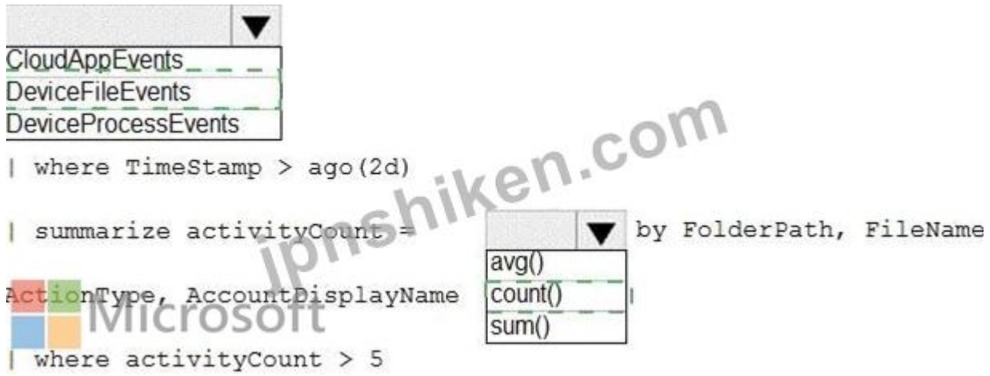
質問: **1**
次のインシデントを含む Microsoft Sentinel ワークスペースがあります。
Azure Portal 分析ルールに対するブルート フォース攻撃がトリガーされました。
インシデントに対応する地理位置情報を特定する必要があります。
あなたは何をするべきか？
A. [概要] から、[潜在的な悪意のあるイベント] マップを確認します。
B. インシデントから、インシデントに関連付けられた iPCustomEntity エンティティの詳細を確認します。
C. インシデントから、インシデントに関連付けられた AccouncCuscomEntity エンティティの詳細を確認します。
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: **A** (コメントを発表する)

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

質問: **2**
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。



正解:



Explanation:

Table: DeviceFileEvents

Aggregation function: count()

In Microsoft Defender XDR advanced hunting, data tables such as DeviceFileEvents , DeviceProcessEvents , and CloudAppEvents are used to investigate various types of activities. Since this query aims to investigate an issue related to file activity-specifically identifying when files have been accessed, modified, or created repeatedly-the correct data source table is DeviceFileEvents . This table contains information about file- level activities recorded by Defender for Endpoint sensors, including file path, file name, action type, and user account involved.

The KQL structure shown in the image follows standard hunting query syntax:

DeviceFileEvents

| where Timestamp > ago(2d)

| summarize activityCount = count() by FolderPath, FileName, ActionType, AccountDisplayName

| where activityCount > 5

Here's why:

* The where Timestamp > ago(2d) clause filters results from the last 2 days, a typi cal timeframe for immediate investigations.
* The summarize operator groups events by FolderPath, FileName, ActionType, and AccountDisplayName, then uses count() to determine how many times each file was acted upon.
* Finally, where activityCount > 5 filters t o show only unusually high-frequency activity, which might indicate suspicious or automated file manipulation.

Microsoft Defender XDR documentation highlights that DeviceFileEvents is the correct schema for file activity investigations, while DeviceProcess Events focuses on process creation and execution, and CloudAppEvents targets cloud application usage.

Thus, the verified and documented correct completions are:

Table: DeviceFileEvents

Aggregation function: count()

質問**: 3**

SW1という名前のMicrosoft Sentinelワークスペースがあります。

SW1でどの異常検知ルールが有効になっているかを特定する必要があります。

Microsoft Sentine1では、何をレビューすべきでしょうか？

A. 設定

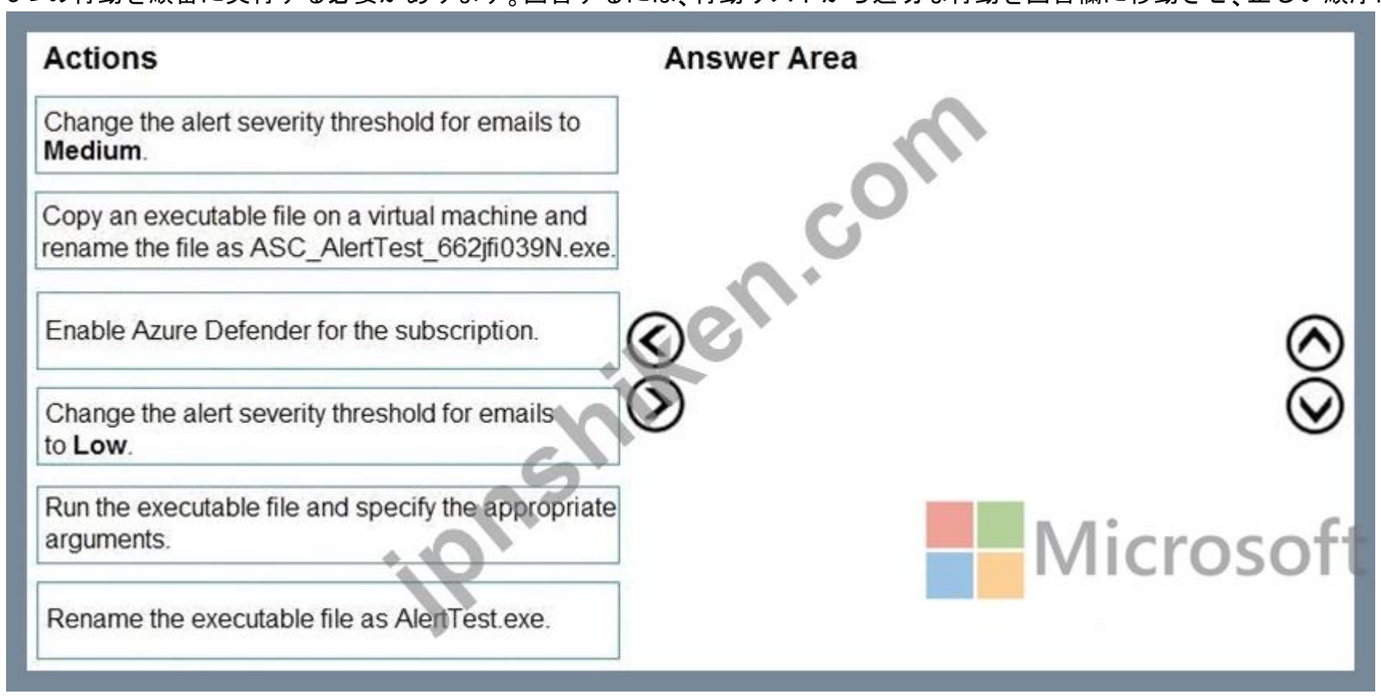
B. エンティティの振る舞い

C. 分析

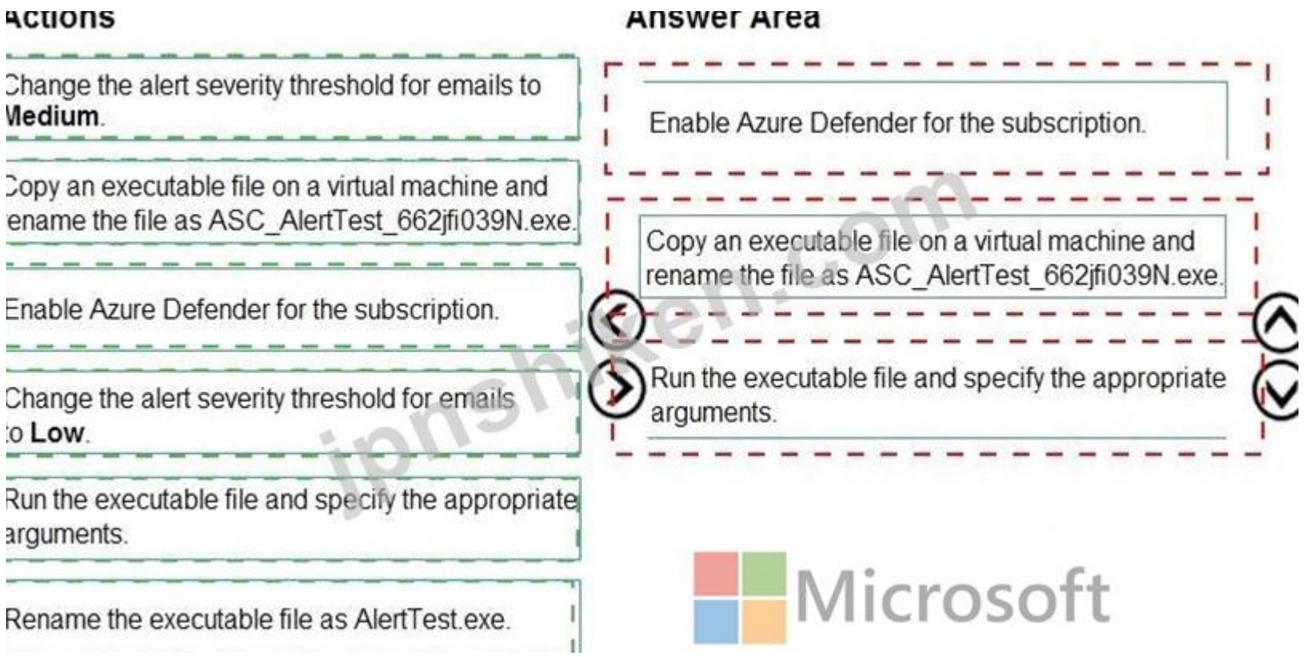
D. コンテンツハブ

正解: (正解を表示します)
To identify which anomaly rules are enabled in a Microsoft Sen tinel workspace (here, SW1), you look at the Sentinel analytics configuration in the portal. In Microsoft's documentation "Work with anomaly detection analytics rules in Microsoft Sentinel," it explains:
"You can now find anomaly rules displayed in a grid in the Anomalies tab in the Analytics page. ... On the Analytics page, select the Anomalies tab. ... Status - whether the rule is enabled or disabled."
Microsoft Learn Thus, anomaly detection rules are a subtype of analytics rules in Sentinel, and they are surfaced under the Analytics area (in the Anomalies tab). That is where you can review which anomaly detection rules are active (enabled) or not.
By contrast:
* Settings is used for workspace-wide configurations (e.g. enabling UEBA, toggling anomalies on/off).
* Entity behavior is a separate feature (UEBA) for monitoring entities and their behavioral baselines, not the repository of which anomaly rules are enabled.
* Content hub is the repository of shared analytics templates and solutions you can import; it does not list which rules are enabled in your workspace.
Therefore, the correct place to review enabled anomaly detection rules is C. Analytics (speci fically under the Anomalies tab).

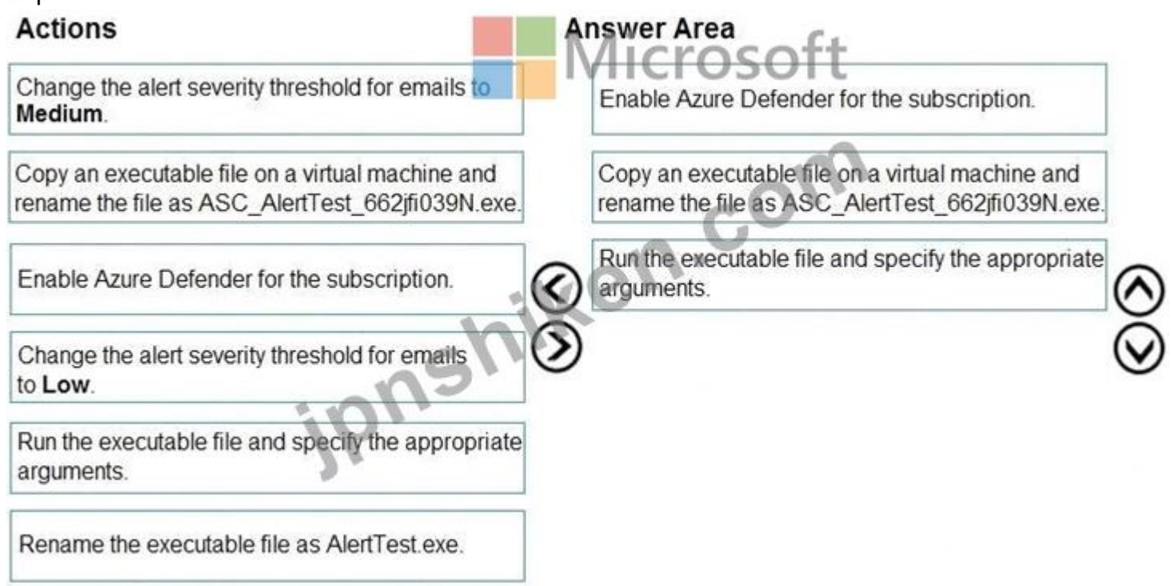
質問: **4**
新しいAzureサブスクリプションを作成し、Azure Monitor用のログの収集を開始します。
Azure Security Center を構成して、疑わしい IP アドレスから Azure 仮想マシンへのサインインに関連する潜在的な脅威を検出できるようにする必要があります。ソリューションは、この構成を検証する必要があります。
3つの行動を順番に実行する必要があります。回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



According to Microsoft Security Operations and Azure Defender (now Microsoft Defender for Cloud) documentation, to validate that Azure Security Center (ASC) - or Defender for Cloud - is properly configured to detect threats such as sign-ins from suspicious IP addresses , you must enable Defender for the subscription first. This step activates the advanced threat protection features that analyze security signals from Azure resources, including virtual machines and network connections.

Once enabled, Microsoft provides a test alert validation process using a PowerShell script or an executable test file to simulate an alert. The official procedure states that to test the alert generation capability, administrators should copy a provided executable file to a virtual machine onboarded to Defender and rename the file using the naming convention beginning with ASC_AlertTest_ followed by random characters. This allows Defender for Cloud to recognize it as a test event.

After renaming, the executable is run with appropriate arguments to trigger a benign test alert that validates Defender's detection pipeline. This alert verifies that the system correctly monitors VM activity and reports potential threats.

Changing alert severity or renaming files differently does not validate the configuration. Therefore, the correct sequence-confirmed by Microsoft documentation-is:
* Enable Azure Defender for the subscription.
* Copy and rename the alert test file (ASC_AlertTest_...).
* Run the executable file with required arguments to trigger and validate detection.

質問: **5**
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のループバック期間は12時間です。
ループバック期間を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. 周波数
B. KQLクエリの要約演算子
C. KQLクエリのwhere演算子
D. スコープ
正解: **(**正解を表示します**)**
XDR Custom Detection Rules Documentation):
In Microsoft Defender XDR, custom detection rules are scheduled KQL queries that evaluate telemetry on a recurring schedule, using a lookback (loopback) period to determine how much historical data to analyze during each run.
The loopback period determines the time window over which data i s evaluated (e.g., 12 hours, 48 hours). To change this period, administrators modify the rule's schedule configuration - specifically the frequency or recurrence settings in the custom detection rule editor. The KQL query (including summarize or where oper ators) defines the logic but not the temporal scope of data evaluation.
Therefore, extending the loopback from 12 hours to 48 hours requires adjusting the frequency (schedule) configuration of the rule, not the query itself.
Correct Answer: A. the freque ncy

質問: **6**
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: Azure Identity Protection から、サインイン リスク ポリシーを構成します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
Azure Identity Protection is used to detect and remediate risky sign-ins based on user behavior and risk levels, but it does not configure decoy or Honeytoken accounts. Honeytoken accounts are a Defender for Identity feature, not an Identity Protection feature.
The solution described (configuring sign-in risk policies in Azure Identity Protection) relates to conditional access and risk-based sign-in responses, not to creating monitored decoy accounts.
Hence, the goal of configuring several accounts for attacker exploitation (Honeytoken monitoring) is not met by this solution.

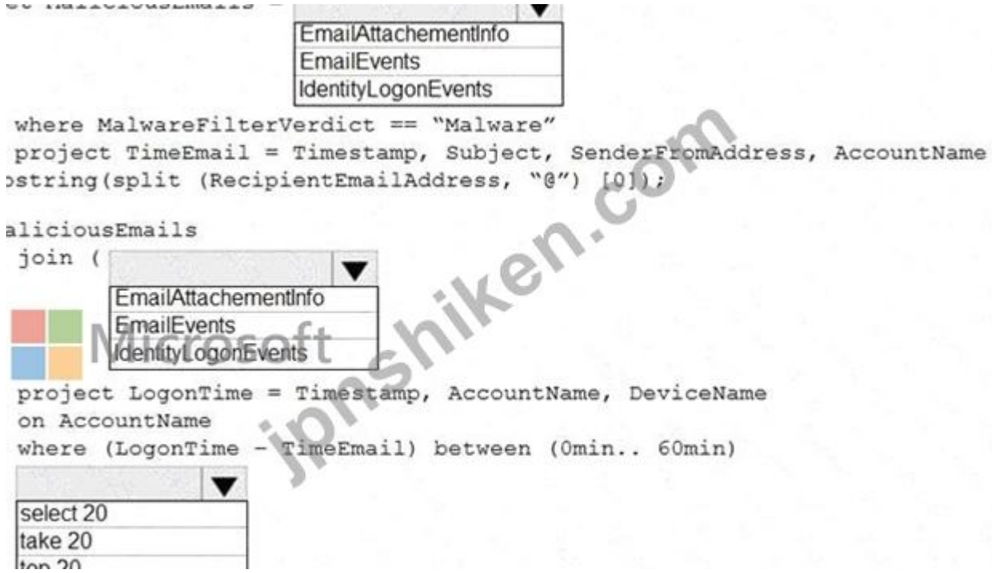
質問: **7**

イメージ ファイルを使用した潜在的な攻撃に関するセキュリティ情報を受け取ります。
攻撃を防ぐには、Microsoft Defender for Endpoint で侵害インジケーター (IoC) を作成する必要があります。
どのタイプのインジケーターを使用する必要がありますか?
A. アクションがアラートのみに設定されている URL/ドメイン インジケーター
B. アクションがアラートとブロックに設定されている URL/ドメイン インジケーター
C. アクションがアラートとブロックに設定されているファイル ハッシュ インジケーター
D. アクションがアラートとブロックに設定されている証明書インジケーター
正解: **(**正解を表示します**)**
According to Microsoft Defender for Endpoint documentation, Indicators of Compromise (IoCs) can be created based on file hashes, IPs, URLs/domains, or certificates . When the bulletin references a potential attack that uses an image file , it implies that the malicious component is a specific file type (e.g., .jpg , .png , .
ico) being weaponized.
The appropriate IoC for file-based threats is a File hash indicator . You create this indicator by specifying the hash (SHA-1, SHA-256, or MD5) of the suspicious file and setting its Action to "Alert and block" , which ensures that Defender for Endpoint both raises an alert and prevents execution of the file on protected endpoints.
From Microsoft documentation:
"You can create indicators for file hashes, IP addresses, URLs/domains, and certificates. When creating file hash indicators, set the action to Alert and block to prevent execution of known malicious files on endpoints." Other options explained:
* A & B (URL/domain) - These are used for blocking malicious websites or command-and-control domains, not image files.
* D (Certificate) - Used for detecting or blocking applications signed with malicious certificates, not for specific file-based threats.
# Correct Answer: C. a file hash indicator that has Action set to Alert and block

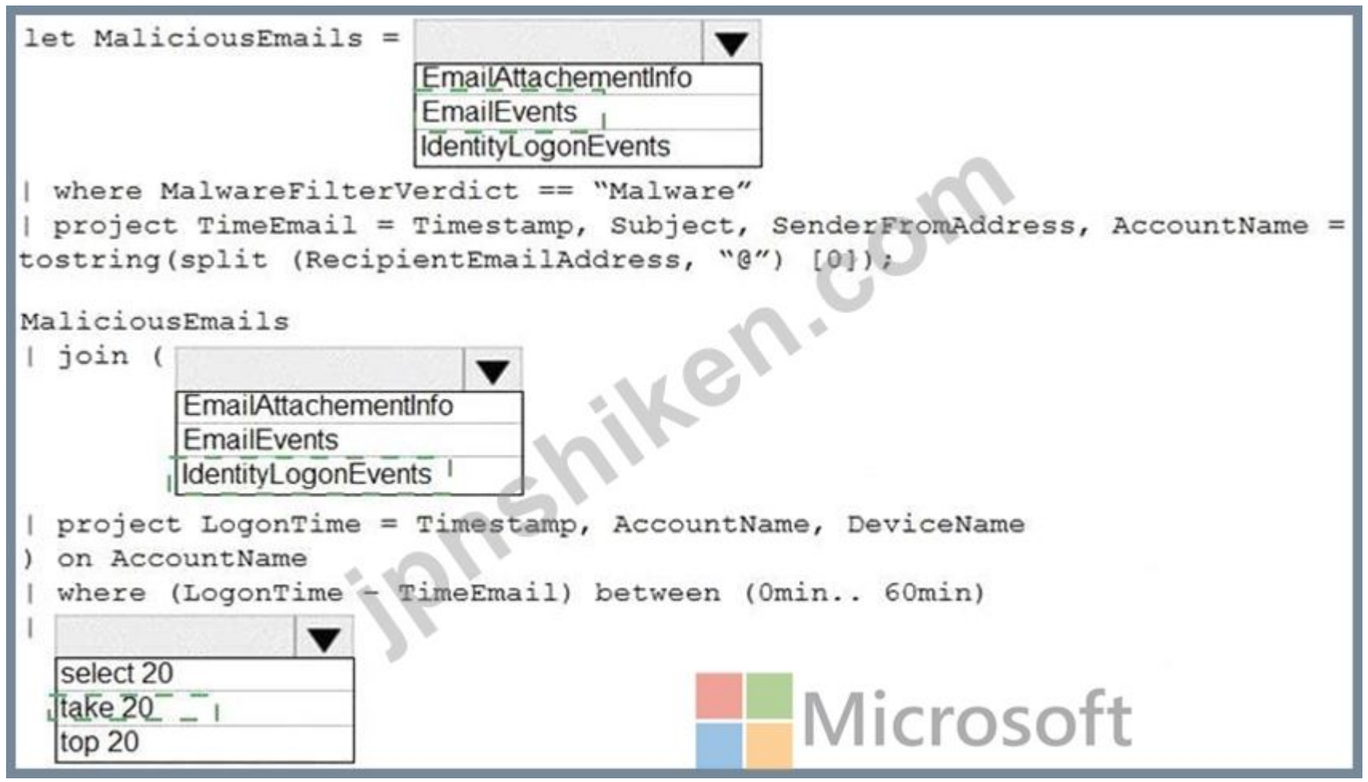
質問: **8**
技術要件を満たすためには、現在発生している攻撃に対処する必要があります。
解決策には何を含めるべきですか？
A. Azure Automation ランブック
B. Azure Logic Apps
C. Azure Functions
D. Azure Sentinel のライブストリーム
正解: **(**正解を表示します**)**
To remediate active attacks automatically once alerts or incidents are detected, Microsoft Sentinel uses playbooks , which are workflows built on Azure Logic Apps . These playbooks can execute remediation actions-such as isolating a machine, blocking an account, or triggering other security control chang es- without manual intervention. Microsoft's documentation clearly states that "playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps" and that they can "automate and orchestrate your threat response by using playbooks ... run a pla ybook on-demand or automatically in response to specific alerts or incidents." When an analytics rule in Sentinel triggers an alert or incident, you can attach an automation rule which in turn invokes a playbook (i.e. a Logic Apps workflow) to perform the remediation steps. The automation rule defines the trigger conditions and calls the playbook action as part of its response actions.
Let us evaluate other options:
* Azure Automation runbooks (Option A) are powerful for scripting in Azure (e.g., PowerShell o r Python) and can perform remediation tasks, but they are not the native mechanism within Sentinel for orchestrated, alert-driven response workflows.
* Azure Functions (Option C) are serverless compute for custom code, but you would have to build and integra te orchestration logic manually; they are not the out-of-box SOAR component in Sentinel.
* Azure Sentinel livestreams (Option D) is not a recognized remediation automation component-it is irrelevant in this context.
Therefore, the correct solution to remedia te active attacks (triggering automated actions in response to alerts
/incidents with minimal manual effort) is to use Azure Logic Apps (via Sentinel playbooks) as the orchestration engine. Logic Apps are the documented foundation of Sentinel's automation r esponse capabilities.

質問: **9**
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. Microsoft Cloud Security Benchmark (MCSB) の割り当てを無効にします。
C. Azure Event Hubs の継続的エクスポート設定を構成します。
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**)**
In Micro soft Defender for Cloud, regulatory compliance standards such as PCI DSS 4.0 , ISO 27001 , and NIST SP 800-53 are part of the Cloud Security Posture Management (CSPM) capabilities. To assign or view these regulatory initiatives, the CSPM plan must first be e nabled for the environment.
According to Microsoft Defender for Cloud documentation, when you open Environment settings # Security policy , you can view and manage the assigned initiatives. If the option to "Add more industry and regulatory standards" is gr ayed out or unavailable , it means that the CSPM plan is not active for that subscription.
Once you enable the Defender CSPM plan , Defender for Cloud automatically assigns the Microsoft Cloud Security Benchmark (MCSB) initiative and allows you to add additi onal frameworks such as PCI DSS 4.0, NIST, or SOC 2.
* Option A (Correct) - Enabling CSPM unlocks regulatory compliance capabilities, allowing you to assign the PCI DSS 4.0 initiative.
* Option B - Disabling MCSB is unnecessary and not required; it's automatically included when CSPM is enabled.
* Options C and D - Continuous export settings (to Event Hubs or Log Analytics) are used for exporting data, not enabling compliance initiatives.
Hence, the first step to make the "Add more standards" option avail able is to enable the Cloud Security Posture Management (CSPM) plan on the subscription.

質問: **10**
ユーザーの皆様が受信する悪質なメールが増加していることをお知らせいたします。
メール受信者のアカウントが侵害されたかどうかを特定するには、Microsoft 365 Defender で高度なハンティングクエリを作成する必要があります。このクエリは、既知の悪意のあるメールを受信してから 1 時間以内に受信者が行った最新のサインイン 20 回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:

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

質問: 11

Microsoft Defender XDR のカスタム検出ルールに、以下の KQL クエリが含まれています。

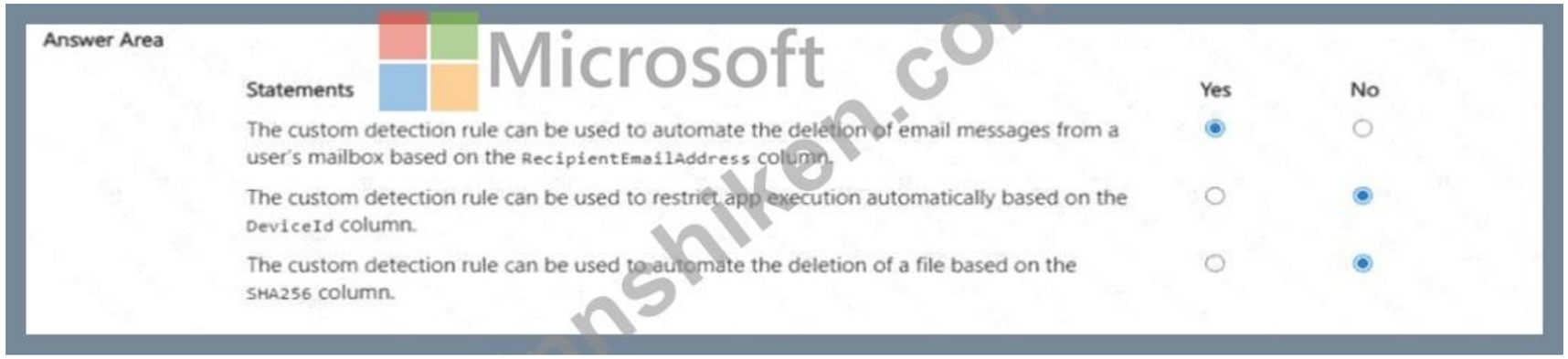
```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId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

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

注：正解ごとに1ポイントが加算されます。

正解:

Explanation:



質問: **12**

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。

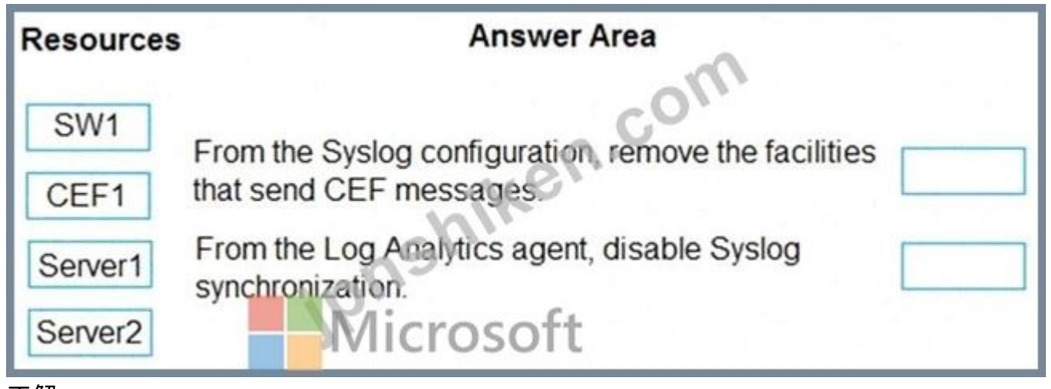
D. キー コンテナーのアクセス ポリシーを変更します。

正解: (正解を表示します)
When Azure Defender for Key Vault (now part of Microsoft Defender for Cloud) raises an alert about suspicious access attempts from multiple unknown IP addresses, the immediate mitigation step-before deeper investigation-is to restrict network access to the Key Vault to reduce exposure.
The Azure Key Vault firewall allows you to restrict access by:
* Allowing access only from trusted IP addresses, VNets, or private endpoints.
* Blocking all other traffic by enabling the firewall and disabling "Allow access from all networks." Microsoft's official recommendation states:
"To reduce the likelihood of secrets being compromised while you investigate an alert, enable the Key Vault firewall and restrict access to trusted networks or specific virtual networks."
"Firewall and virtual network configuration can be applied immediately without affecting existing permissions or access policies." This step:
* Minimizes exposure to malicious IP addresses.
* Is quick to implement (through the Azure Portal or CLI).
* Has minimal impact on legitimate users if you properly whitelist trusted networks or VNets.
Other options:
* A (Modify access control settings) or D (Modify access policy) would affect permissions and could disrupt legitimate users or service principals.
* C (Create an application security group) applies to network interfaces, not directly to Key Vault.
# answer: B. Enable the Key Vault firewall

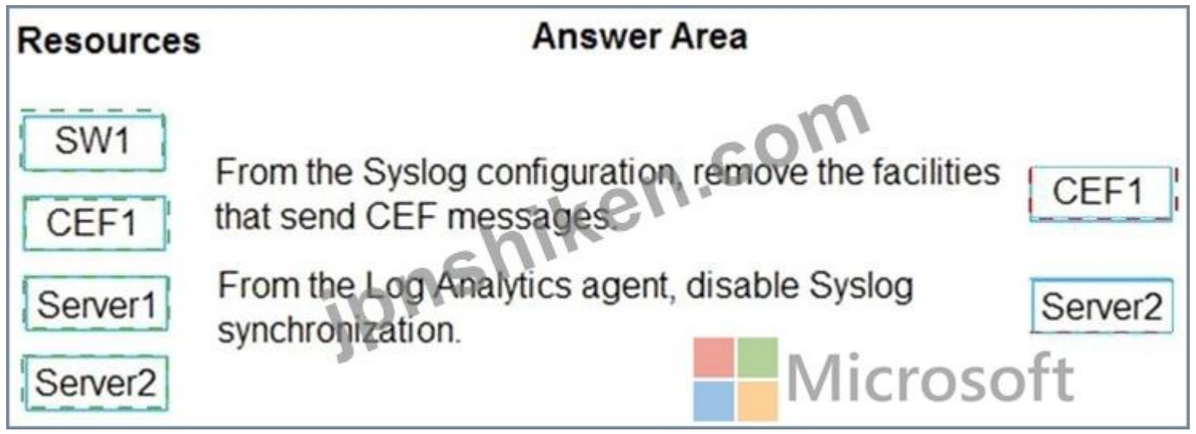
質問: **13**
以下の表に示すリソースが利用可能です。

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。



正解:



Explanation:

| From the Syslog configuration, remove the facilities that send CEF messages. | CEF1 | | From the Log Analytics agent, disable Syslog synchronization. | Server2 | The goal is to eliminate duplicate events in the Azure Sentinel workspace (SW1). Duplication typically occurs when the same log source is sending data to Azure Sentinel via multiple collection methods .

Analysis of the Environment

* SW1 is the Azure Sentinel (now Microsoft Sentinel) workspace, which is the final destination for all logs.
* CEF1 is a Linux server configured as a log forwarder (often called a CEF collector) for Microsoft Sentinel. It uses the Log Analytics agent (or the newer Azure Monitor Agent) to ingest logs and is specifically configured to forward Common Event Format (CEF) logs to SW1 .
* Server1 sends CEF logs to CEF1 . This is the intended, single collection path for Server1 ' s CEF logs:

Server1 CEF1 SW1. No duplication is inherent here.

* Server2 sends Syslog logs to CEF1 . This path is: Server2 CEF1 SW1.
* Since CEF1 is running the Log Analytics agent (required to forward logs to SW1) and is configured to collect Syslog data (to receive Server2 ' s logs), the Log Analytics agent on CEF1 will also attempt to ingest the Syslog messages it receives into SW1.
* However, the Log Analytics agent itself can also be used to collect Syslog/CEF logs directly from the source server.

Addressing Duplication

Duplication is most likely to occur if a server is sending the same logs to a forwarder AND also has the Log Analytics agent configured to send the same logs directly to SW1.

Action 1: From the Syslog configuration, remove the facilities that send CEF messages.

* Resource: CEF1
* Reasoning: CEF1 is a Linux server running the Log Analytics agent and is acting as the collector.

Server1 sends CEF logs to CEF1. These CEF logs are transmitted using Syslog (specifically, a custom Syslog format). If the Log Analytics agent on CEF1 is configured to collect all Syslog facilities, it will ingest the raw CEF Syslog messages it receives from Server1 AND also ingest the parsed CEF messages via its custom forwarding logic. To prevent the Syslog collector on CEF1 from ingesting the raw CEF messages that it is supposed to be forwarding , you must modify its Syslog configuration (e.

g., in /etc/rsyslog.conf or equivalent) to ignore the facilities/log files used by the incoming CEF messages from Server1. The primary purpose of CEF1 is to receive and forward CEF, not to have its Log Analytics agent ingest the raw Syslog that transports the CEF payload.

Action 2: From the Log Analytics agent, disable Syslog synchronization.

* Resource: Server2
* Reasoning: Server2 is configured to send Syslog logs to CEF1 (Server2 CEF1 SW1). Since Server2 is a Linux server, it may also have the Log Analytics agent installed for other monitoring purposes. If the Log Analytics agent on Server2 is installed, it is configured by default to collect Syslog logs directly and send them to SW1 (Server2 SW1). This creates a duplicate path for the Syslog data:
* Path A (Intended): Server2 Syslog CEF1 SW1
* Path B (Duplication): Server2 Log Analytics Agent Syslog SW1

* According to Microsoft Sentinel documentation on log ingestion, when using a dedicated forwarder (like CEF1) for Syslog/CEF, you must disable the Syslog collection on the Log Analytics agent of the source machine (Server2) to prevent this duplication. This is typically done by disabling Syslog synchronization in the Log Analytics agent configuration or removing the Syslog entry from the agent ' s data sources.
References: Microsoft Sentinel documentation on data connectors for Syslog and CEF, specifically the sections discussing the deployment of the Log Analytics agent and forwarders, which repeatedly warn about the need to prevent dual-ingestion of the same log type (Syslog or CEF) from both the source server ' s agent and a dedicated collector/forwarder.

質問**: 14**
Microsoft Defender for Servers Plan 1 を使用し、Server1 という名前のサーバーを含む Azure サブスクリプションがあります。
エージェントレス スキャンを有効にします。
Server1 がスキャンされないように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。
あなたは何をするべきか？
A. 除外タグを作成します。
B. サブスクリプションを Defender for Servers プラン 2 にアップグレードします。
C. ガバナンス ルールを作成します。
D. 除外グループを作成します。
正解**: (**正解を表示します**)**
With Defender for Servers Plan 1 or Plan 2 , agentless scanning for vulnerabilities is enabled to assess connected servers automatically. To exclude specific servers (like Server1) from being scanned, Microsoft recommends using exclusion tags .
An exclusion tag is a key-value metadata pair (for example, DefenderForCloud.AgentlessScan = Exclude) applied to resources to exclude them from certain Defender for Cloud assessments, including agentless vulnerability scanning. This approach is lightweight and requires no policy or plan upgrade , satisfying the requirement to minimize administrative effort.
Other options explained:
* Upgrade to Plan 2: Not required; exclusion works in Plan 1 and Plan 2.
* Create a governance rule: Used for compliance automation, not scanning exclusions.
* Create an exclusion group: Not a valid Defender for Cloud configuration concept.
# Correct answer: A. Create an exclusion tag

質問**: 15**
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**: B (**コメントを発表する**)**
The Risky users report in Microsoft Entra ID Protection provides visibility into users whose identities might have been compromised. It shows risk levels, risk states, and when risk detections occurred - allowing you to investigate activity for the last 90 days .
The Risk detections report lists individual risk events but not overall user risk status, while risky sign-ins report only sign-in attempts, not the cumulative user risk.
Thus, to determine whether User1's identity was compromised during the last 90 days , use the risky users report .

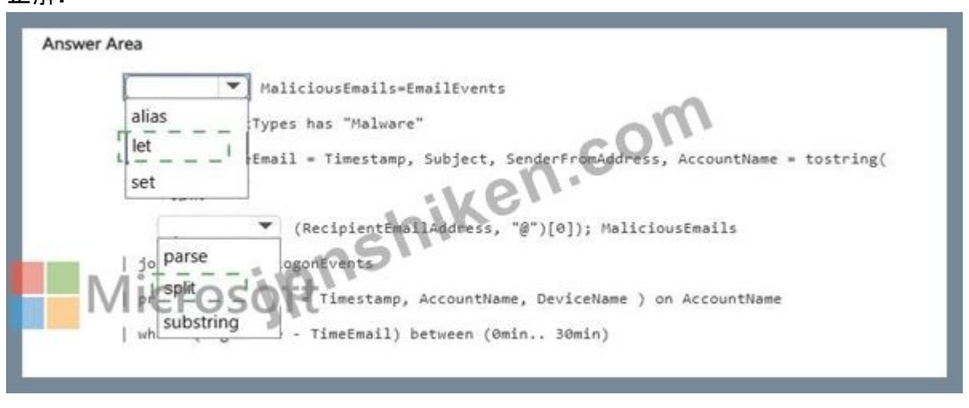
質問: **16**
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用で、User1という名前のユーザーが含まれています。
User1がMicrosoft Defender XDRのカスタム検出ルールとエンドポイントセキュリティポリシーを管理できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1にはどの役割を割り当てるべきですか？
A. デスクトップアナリティクス管理者
B. セキュリティオペレーター
C. セキュリティ管理者
D. クラウドデバイス管理者
正解: **(**正解を表示します**)**
In Microsoft 365 E5 environments that use Microsoft Defender XDR , role-based access control (RBAC) is enforced across the Microsoft Defender portal to align with least-privilege principles. To manage custom detection rules (such as scheduled analytics rules in Defender XDR) and endpoint security policies (such as antivirus, firewall, or attack surface reduction policies in Microsoft Defender for Endpoint), the required role is Security Administrator .
According to Microsoft documentation, the Security Administrator role:
* "Can manage security settings in Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps."
* "Has full permissions to create, edit, and delete security policies, alerts, and detections."
* "Can configure and manage custom detection rules, automated investigation settings, and advanced hunting queries." By contrast:
* Security Operator can view alerts and incidents and take limited response actions but cannot create or manage detection rules or policies.
* Desktop Analytics Administrator relates to Windows analytics and endpoint readiness reporting, not Defender XDR management.
* Cloud Device Administrator primarily manages device onboarding and enrollment in Microsoft Intune or Azure AD, not Defender policies or detections.
Following the principle of least privilege , Security Administrator grants exactly the rights needed to manage Defender XDR custom detection rules and endpoint security policies-without assigning excessive administrative permissions across the tenant.
Therefore, the correct and verified answer is C. Security Administrator .

質問: **17**
サードパーティのセキュリティ情報およびイベント管理 (SIEM) ソリューションを使用しています。
SIEM ソリューションが Azure Active Directory (Azure AD) 署名イベントのアラートをほぼリアルタイムで生成できることを確認する必要があります。
イベントを SIEM ソリューションにルーティングするにはどうすればよいですか?
A. セキュリティ イベント コネクタを備えた Azure Sentinel ワークスペースを作成します。
B. イベント ハブにストリーミングするように Azure AD の診断設定を構成します。
C. Azure Active Directory コネクタを備えた Azure Sentinel ワークスペースを作成します。
D. ストレージ アカウントにアーカイブするように Azure AD の診断設定を構成します。
正解: **(**正解を表示します**)**

According to Microsoft Entra (formerly Azure Active Directory) and Microsoft Security Operations documentation, when integrating Azure AD sign-in logs and audit logs with third-party SIEM systems , the supported and recommended method is to stream the logs to Azure Event Hubs through Diagnostic Settings .
Event Hubs act as a real-time data ingestion service that can integrate directly with external SIEM tools such as Splunk, QRadar, ArcSight, or Sumo Logic. This allows for near real-time alerting and analysis of Azure AD sign-in events.
Official Microsoft guidance states:
"To integrate Azure AD logs with third-party SIEMs, configure Azure AD Diagnostic Settings to send sign-in and audit logs to Azure Event Hubs. Event Hubs can then stream the data to your SIEM for near real-time monitoring." Other options do not meet the scenario's requirement:
* (A) and (C) involve Azure Sentinel, Microsoft's native SIEM solution. Since the question specifies a third-party SIEM , Sentinel is not required.
* (D) Archiving to a Storage account provides long-term retention and offline analysis but does not support near real-time alerting.
Therefore, the correct approach to route Azure AD sign-in events for near real-time monitoring in a third- party SIEM is to configure Azure AD Diagnostic Settings to stream logs to an Azure Event Hub .
Correct Answer: B. Configure the Diagnostics settings in Azure AD to stream to an event hub

質問**: 18**
あなたはMicrosoft 365のサブスクリプションをお持ちです。
あなたはMicrosoft Defender XDRを使用して、メール関連の脅威を検出する予定です。
既知の悪意のあるメールをユーザーが受信してから30分以内に行われた、ユーザーによるサインイン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:



Explanation:

質問: **19**
Azure Sentinel を構成しています。
サインイン リスク イベントを表すインシデントが Azure Sentinel でアクティブ化されるたびに、Microsoft Teams メッセージをチャネルに送信する必要があります。
Azure Sentinel で実行する必要がある 2 つのアクションはどれですか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. エンティティの動作分析を有効にします。
B. インシデントをトリガーした分析ルールにプレイブックを関連付けます。
C. Fusion ルールを有効にします。
D. プレイブックを追加します。
E. ワークブックを作成します。
正解: **B,D (コメントを発表する)**
To automatically send a Microsoft Teams message when an incident (like a sign-in risk) is activated, you must use Logic Apps playbooks in Microsoft Sentinel.
Steps based on Microsoft documentation:
* Add (create) a playbook (Option D) - a Logic App workflow that defines the automation (e.g., post a message to a Teams channel).
* Associate the playbook to the analytics rule (Option B) that generates the incident - this ensures the playbook triggers automatically whenever that rule fires.
Other options do not accomplish the goal:
* Entity behavior analytics (A) provides user and entity context but does not automate actions.
* Fusion rule (C) correlates multi-stage attacks automatically but isn't used to trigger notifications.
* Workbooks (E) are for visualization, not automation.
# Final Answers:
* Question 80: D. Assign the incident
* Question 83: B and D

質問: **20**
次の環境があります。
アズールセンチネル
Microsoft 365 サブスクリプション
ID 用の Microsoft Defender

Azure Active Directory (Azure AD) テナント
すべての Active Directory メンバー サーバーとドメイン コントローラーからセキュリティ ログを収集するように Azure Sentinel を構成します。
Microsoft Defender for Identity は、スタンドアロン センサーを使用して展開します。
Active Directory で機密グループがいつ変更されたかを確実に検出できるように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. ドメイン コントローラーの詳細監査ポリシー構成設定を構成します。
B. ドメイン コントローラー組織単位 (OU) のアクセス許可を変更します。
C. Microsoft 365 コンプライアンス センターで監査を構成します。
D. ドメイン コントローラーで Windows イベント転送を構成します。
正解: **A,D (**コメントを発表する**)**
Microsoft Defender for Identity (MDI) detects sensitive group modifications-such as changes to Domain Admins, Enterprise Admins, or Schema Admins-by analyzing Windows security events from domain controllers. For MDI sensors to detect such changes, advanced audit policies must be configured to log these activities (specifically Directory Service Changes and Account Management events).
Microsoft documentation specifies that "Defender for Identity requires auditing to be enabled on domain controllers for security events like group membership changes." This is done under Advanced Audit Policy Configuration # Directory Service Changes.
Additionally, Windows Event Forwarding (WEF) is required or beneficial when Azure Sentinel needs to centralize those events from multiple domain controllers into a Log Analytics workspace. WEF minimizes administrative effort by automatically collecting logs without manual export or per-server log pulling.
Thus, configuring Advanced Audit Policy ensures the right events are generated, and Windows Event Forwarding ensures those events reach Sentinel for correlation with MDI alerts.
Correct Answers: A and D

質問: **21**
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。すべてのエンドポイント デバイスは、Microsoft Defender for Endpoint にオンボーディングされています。
Azure サブスクリプションには、Workspace 1 という名前の Microsoft Sentinel ワークスペースが含まれています。すべての Microsoft Defender XDR イベントは Workspace1 に取り込まれます。
お客様はMicrosoft Entraテナントをお持ちです。
既知の脆弱性をデバイスログから検索する、query1という名前のKQLクエリを作成します。
クエリ1が1時間ごとに実行され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。
何を設定すればよいですか？
A. 自動化ルール
B. 自動調査および対応(AIR)
C. ウォッチリスト
D. カスタム検出ルール
正解: **D (**コメントを発表する**)**
To have your query1 run every hour in a Microsoft Sentinel environment, you should configure it as an analytics rule-specifically a scheduled query (custom detection) rule . Microsoft's official documentation for Sentinel describes "scheduled analytics rules" as queries that you configure to run on a recurring schedule, with a defined lookback period, and trigger alerts if the query results meet the rule criteria. Those scheduled rules are the mechanism by which KQL queries are periodically executed automatically.
When you create an analytics rule in Sentinel, you supply the query (i.e. query1) and you specify the recurrence (for example, every hour). Once configured as such, Sentinel takes care of executing it on schedule with minimal ongoing administrative intervention. This aligns exactly with "minimize administrative effort." Among the answer choices:
* An automation rule is used to act upon alerts (for example, route, suppress, or apply playbooks) but does not itself schedule periodic queries.
* Automated Investigation and Response (AIR) is part of Defender for Endpoint's automated remediation workflow and is used for responding to alerts on endpoints-not for scheduling general KQL hunting queries.

* A watchlist is a static data reference (list of values) you can use within queries or rules but does not itself execute queries on a schedule.
* A custom detection (analytics) rule is exactly what you would use to wrap query1 into a scheduled operation.
Thus, converting query1 into a custom detection rule (i.e. a scheduled analytics rule) is the correct choice.
From Microsoft SecOps and Sentinel rule documentation: scheduled rules are based on Kusto queries configured to run at regular intervals over a lookback period, and if results cross a threshold, an alert is triggered. The rule's scheduling frequency (such as hourly) is part of rule configuration. This model ensures your query1 gets executed every hour automatically with minimal manual work.

質問**: 22**
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**: 23**
デフォルトのデータ保持期間が30日間に設定されているMicrosoft Sentinelワークスペースがあります。このワークスペースには、次の表に示す2つのカスタムテーブルが含まれています。

Name	Table plan	Interactive retention	Total retention period
Table1	Basic	Default	Default
Table2	Analytics	Default	365

過去365日間、各テーブルは1日あたり2件のレコードを取り込んだ。
分析ルールで使用するKQLステートメントは、次の表に示すように作成します。

Name	KQL statement
Query1	Table1 | where TimeGenerated >= ago(15) | summarize count()
Query2	Table2 | where TimeGenerated >= ago(120) | summarize count()
Query3	Table1 | where TimeGenerated >= ago(45)

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
For Query1 to return a value of 30, you must change Table plan to **Analytics**.	○	○
For Query2 to return a value of 240, you must change Total retention period to **120 days**.	○	○
For Query3 to return 90 rows, you must change Total retention period to **45 days**.	○	○

正解:

Answer Area

Statements	Yes	No
For Query1 to return a value of 30, you must change Table plan to **Analytics**.	○	○
For Query2 to return a value of 240, you must change Total retention period to **120 days**.	○	○
For Query3 to return 90 rows, you must change Total retention period to **45 days**.	○	○

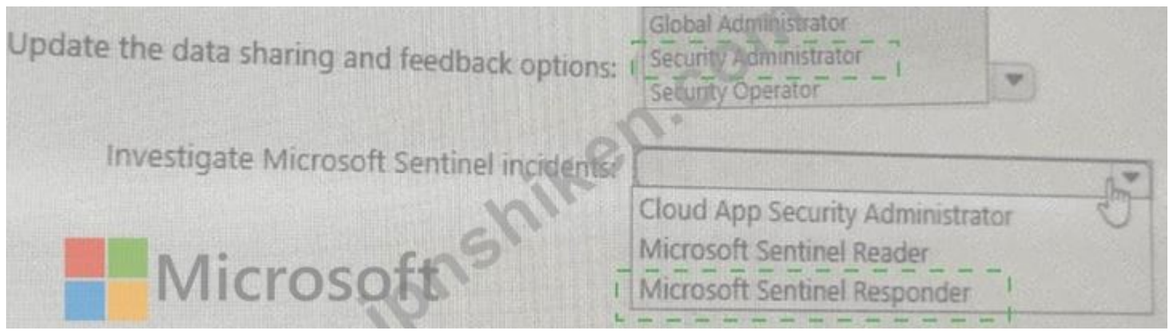
質問: **24**
Azure仮想マシンの技術要件を満たすソリューションを提案する必要があります。提案には何を含めるべきでしょうか？
A. ジャストインタイム (JIT) アクセス
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway
正解: **(**正解を表示します**)**
Reference:
To meet the requirement "Receive alerts if an Azure virtual machine is under brute force attack," you should enable Azure Defender (now Microsoft Defender for Cloud plans for Servers). Defender continuously collects and analyzes security telemetry from your VMs (RDP/SSH sign-in attempts, process and network signals, and OS logs) and raises security alerts for patterns that in dicate attacks such as RDP/SSH brute force . These alerts include rich context (attacked host, source IPs, timeframe, and recommended remediation) and natively integrate with Microsoft Sentinel , allowing incidents, automation rules, and playbooks to be trig gered with minimal administration.
While Just-in-Time (JIT) VM access is an important hardening control-also provided through Defender for Cloud-it primarily reduces exposure by closing management ports and opening them only on request; it does not itself generate analytics-based brute-force alerts . Azure Firewall and Azure Application Gateway are perimeter controls (L3-L7 filtering and web application firewall, respectively) and do not provide host- level brute-force detection on VM sign-ins.

Therefore, the solution that directly satisfies the technical requirement to detect and alert on brute-force activity against Azure VMs -and integrates seamlessly with Sentinel for rapid remediation-is Azure Defender (Microsoft Defender for Cloud) .
Reference: Microsoft D efender for Cloud documentation on VM threat protection and brute-force (RDP /SSH) detection and alerting, and integration with Microsoft Sentinel for incident creation and response.

質問: **25**
Server1 のイベント監視を設定する必要があります。ソリューションは Microsoft Sentinel の要件を満たす必要があります。最初に何を作成すればよいでしょうか？
A. Microsoft Sentinel 自動化ルール
B. Microsoft Sentinel スケジュール済みクエリ ルール
C. データ収集ルール(DCR)
D. Azure Event Grid トピック
正解: **C (コメントを発表する)**
To monitor Windows Security events from Server1 using the Windows Security Events via AMA connector, the first object you must create is a Data Collection Rule (DCR) . With the Azure Monitor Agent (AMA) model used by Microsoft Sentinel, data flow is controlled by DCRs, not by the legacy MMA/OMS workspace settings. A DCR defines what to collect (e.g., the Security event log, specific event IDs or XPath queries), from where (the target machines or machine groups), and where to send it (the Sentinel/Log Analytics workspace). After creating the DCR, you associate it with Server1 (Arc-enabled), and the connector will begin streaming Security events to your Sentinel workspace. Creating a Sentinel sch eduled rule or an automation rule does not enable collection; those features act after data is already ingested. Event Grid topics are unrelated to Windows event collection. Therefore, the correct first step for meeting the Sentinel requirement to monitor Server1's Security log via AMA is to create a DCR , then assign it to Server1 and the Sentinel workspace.

質問: **26**
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ポイント獲得できます。

正解:



Explanation:
Task
Role
Update the data sharing and feedback options
Security Administrator
Investigate Microsoft Sentinel incidents
Microsoft Sentinel Responder
Microsoft Sentinel built-in roles documentation defines:
Microsoft Sentinel Responder - Can view incidents and perform incident response operations such as assigning, changing severity, or closing incidents.
This role grants the ability to investigate and act on incidents , which includes collaboration with Microsoft Copilot for Security to analyze incidents and run queries within Sentinel.
The Microsoft Sentinel Reader role, on the other hand, can only view incidents but cannot investigate or modify them, making it too restrictive.
The Clou d App Security Administrator role is unrelated to Sentinel incident investigation.
Thus, for investigating Sentinel incidents using Copilot for Security, Microsoft Sentinel Responder is the correct and least-privileged role.
Final Verified Answers: Task
Role to Assign
Update the data sharing and feedback options
Security Administrator
Investigate Microsoft Sentinel incidents
Microsoft Sentinel Responder
* Security Administrator # Required to configure Copilot for Security settings (data sharing & feedback).
* Microsoft Sentinel Responder # Required to actively investigate incidents (least privilege for Sentinel operations).
Summary of Reasoning These align with Microsoft Copilot for Security , Microsoft Sentinel , and Microsoft Entra role-based access contr ol (RBAC) documentation.

質問: **27**
Microsoft Defender for Endpoint を使用する Microsoft 365 E5 サブスクリプションをお持ちの場合、Alertinfo、AlertEvidence、および DeviceLogonEvents テーブルをリンクするクエリを作成する必要があります。このソリューションは、これらのテーブルのすべての行を返す必要があります。
どの通信事業者を利用すべきですか？
A. join kind = inner
B. evaluate hint. Remote =
C. search *
D. union kind = inner

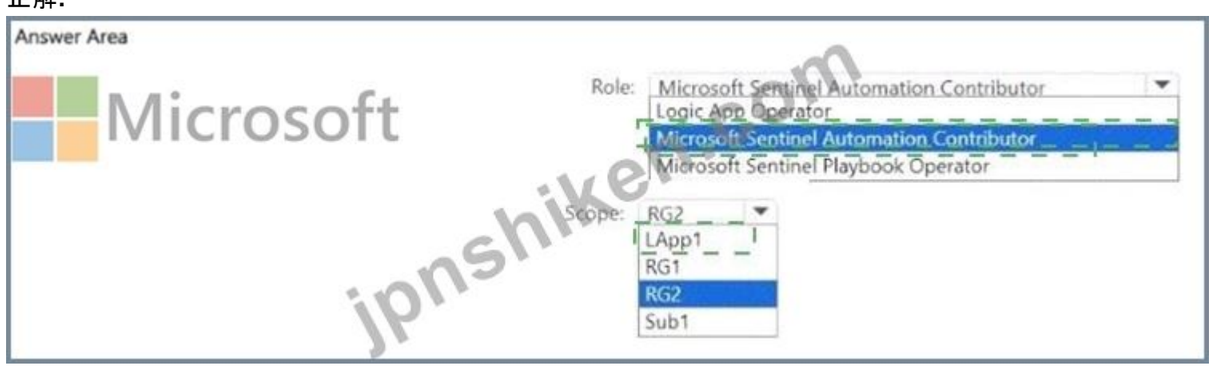
正解: (正解を表示します)
When you need to combine multiple tables (AlertInfo , AlertEvidence , and DeviceLogonEvents) and return all rows from all tables , you use the union operator in KQL (Kusto Query Language).
* join would only return matching records between tables based on a key, not all rows.
* evaluate is used for external function evaluations.
* search * searches across all tables but doesn't create structured combined output.
Using union kind=inner appends results from all three tables while maintaining their structure, allowing you to analyze all alerts, evidence, and logon activity together.
Answer: D. union kind = inner

質問: **28**
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。
Answer Area

正解:



質問: **29**

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ご利用中です。Copilot for Security には既定の設定が構成されています。User1 という名前のユーザーが Copilot for Security を使用して次のタスクを実行できるようにする必要があります。
* ファイルをアップロードしてください。
* 利用状況ダッシュボードを表示します。
* プロンプトブックをすべてのユーザーと共有します。
解決策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. セキュリティ管理者
B. クラウドアプリケーション管理者
C. コパイロット貢献者
D. 副操縦士兼オーナー
正解: **(**正解を表示します**)**
In Microsoft Copilot for Security, permissions are governed by Copilot-specific roles. Copilot Owner is the role designed for administrative stewardship of a Copilot workspace and tenant-level features. According to Microsoft's role definitions, Owners can (1) view usage and billing/consumption dashboards , (2) manage promptbooks , including publishing and sharing promptbooks org-wide so they're available to all users, and (3) control data and session settings , which include allowing users to upload files during sessions.
These capabilities meet all three requirements with a single role and follow least privilege within Copilot's model because it is the lowest rol e that includes both usage visibility and tenant-wide sharing.
By contrast, Copilot Contributor can use Copilot, create prompts, upload files, and create promptbooks, but typically cannot view the usage dashboard and cannot publish/share promptbooks to "ev eryone" across the tenant. Traditional Entra roles such as Security Administrator or Cloud Application Administrator do not grant Copilot for Security workspace administration, usage insights, or promptbook publishing rights.
Therefore, to enable User1 to upload files, view the usage dashboard, and share promptbooks with all users- while using the minimal Copilot role that includes these abilities-the correct choice is Copilot Owner .

質問**: 30**
Azure Security Center が特定のセキュリティ警告を受信したときに自動的に修復処理をトリガーするワークフロー自動化を作成するには、Azure Resource Manager テンプレートを使用する必要があります。
必要な Azure リソースをプロビジョニングするテンプレートの部分はどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

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

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

正解:

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

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Explanation:


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


Microsoft.Automation
Microsoft.Logic
Microsoft.Security

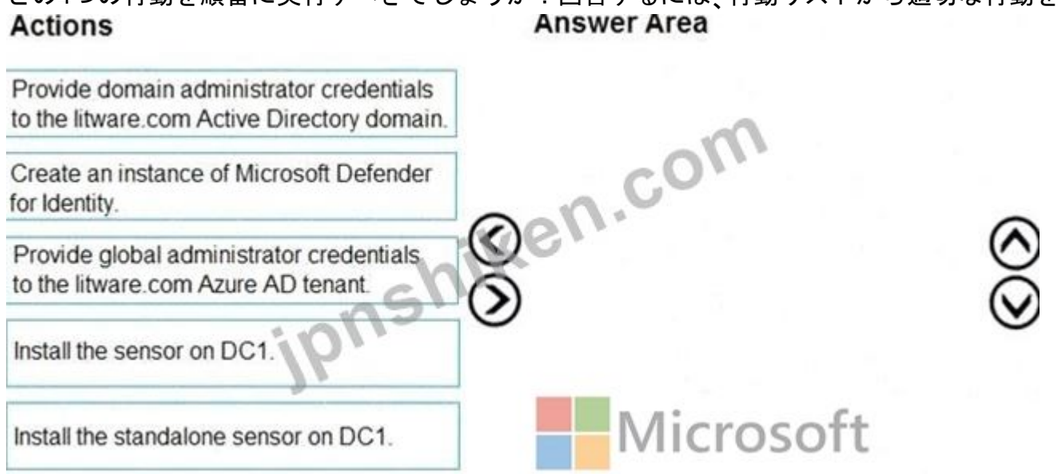
In Azure Security Center (now Microsoft Defender for Cloud), Workflow automation is provisioned as an ARM resource of type Microsoft.Security/automations . The automation resource defines one or more actions , and when the action is a Logic App, the actionType is set to LogicApp and the action must reference the Logic App by its resource ID . In ARM, the correct provider namespace for Logic Apps is Microsoft.Logic , so the template uses resourceId(' Microsoft.Logic/workflows ' , < logicAppName >) to populate logicAppResourceId .
To enable the security alert to trigger the Logic App, the automation action includes a callback URL to the Logic App's manual trigger. In ARM, this is retrieved with listCallbackURL() against the trigger resource ID, which must also use the Microsoft.Logic provider, i.e., resourceId(< subscriptionId > , < resourceGroupName > , ' Microsoft.Logic/workflows/triggers ' , < logicAppName > , ' manual ') , with the Logic Apps API version such as 2019-05-01 . This is the documented pattern for Security Center workflow automations: define an automation under Microsoft.Security/automations , specify an action of type LogicApp , reference the workflow by Microsoft.Logic , and obtain the manual trigger callback via listCallbackURL on Microsoft.Logic/workflows/triggers . This wiring ensures that when the specified security alerts are received, the automation invokes the Logic App for automatic remediation on each match.

質問: **31**
新しい Azure サブスクリプションで Linux 仮想マシンをプロビジョニングします。
Azure Defender を有効にし、仮想マシンを Azure Defender にオンボードします。
仮想マシンに対する攻撃によって Azure Defender でアラートがトリガーされることを確認する必要があります。
仮想マシン上で実行すべき 2 つの Bash コマンドはどれですか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. cp /bin/echo ./asc_alerttest_662jfi039n
B. ./alerttest testing eicar pipe
C. cp /bin/echo ./alerttest
D. ./asc_alerttest_662jfi039n testing eicar pipe
正解: **(**正解を表示します**)**
For Linux alert simulation in Defender for Cloud, you first copy /bin/echo to a test file named asc_alerttest_662jfi039n, then execute it with the parameters testing eicar pipe. This sequence generates a benign test alert that validates the Defender for Cloud pipeline. The options using ./alerttest are incorrect file names and won't trigger the simulation.

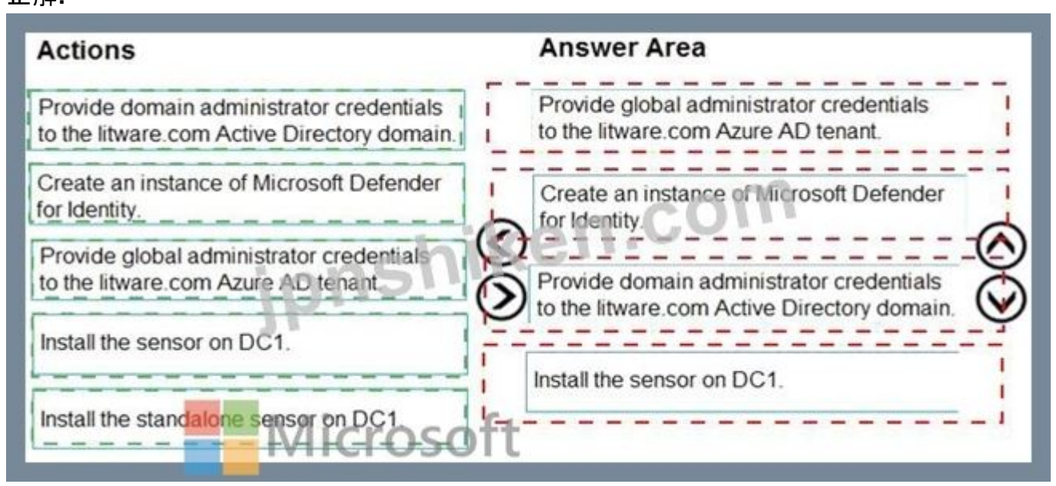
質問: **32**
Microsoft Defender for Cloudを使用するAzureサブスクリプションがあり、その中にUser1という名前のユーザーが存在します。
User1がMicrosoft Defender for Cloudのセキュリティポリシーを変更できるようにする必要があります。このソリューションは、最小権限の原則に基づいている必要があります。
User1にはどの役割を割り当てるべきですか？
A. セキュリティオペレーター
B. セキュリティ管理者
C. 所有者
D. 貢献者
正解: **B (**コメントを発表する**)**
In Microsoft Defender for Cloud's role-based access model, specific Azure built-in roles define what users can view and configure:
* Security Rea der: View-only access to Defender for Cloud recommendations and alerts.

* Security Operator: Can view and dismiss alerts but cannot modify security policies.
* Security Admin: Can view everything a reader can and additionally edit security policies , manage recommendations, and configure settings across Defender for Cloud.
* Owner/Contributor: Have broader Azure resource management rights, exceeding what's required to manage Defender for Cloud policies-violating the principle of least privilege.
The principle o f least privilege dictates assigning the narrowest role that allows performing the required tasks. In this case, the Security Admin role is explicitly documented by Microsoft as granting permission to modify security policies and settings in Defender for C loud, without granting full subscription ownership rights.
Therefore, to allow User1 to modify Defender for Cloud security policies while maintaining least privilege:
Assign the Security Admin role.

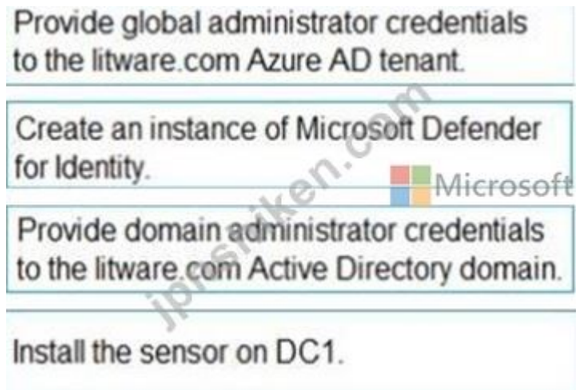
質問: **33**
ビジネス要件を満たすようにDC1を設定する必要があります。
どの4つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



According to Microsoft's official Defender for Identity deployment documentation, setting up Microsoft Defender for Identity (MDI) on an on-premises domain controller (DC) such as DC1 requires a specific sequence of steps. MDI monitors and protects Active Directory from advanced threats by using sensors installed directly on domain controllers.
The correct sequence is as follows:
1# # Provide global administrator credentials to the Azure AD tenant.
Microsoft Defender for Identity is created and managed in the Microsoft 365 Defender portal or Microsoft Security portal, which requires global administrator permissions to provision the MDI instance and connect it to the Azure AD tenant.
2# # Create an instance of Microsoft Defender for Identity.
You must create an MDI instance in the portal before deploying any sensors. This instance defines your Defender for Identity workspace and generates the configuration package that sensors will later use to connect to the cloud service.
3# # Provide domain administrator credentials to the on-premises Active Directory domain.
Domain admin credentials are required for the sensor installation because the sensor must access the domain controller's security logs, event logs, and directory services to monitor authentication traffic and suspicious activities.
4# # Install the sensor on DC1.
Since DC1 is a domain controller connected directly to the internet, the standard sensor (not the standalone sensor) is installed directly on it. The standalone sensor is used only when you do not want to install the sensor directly on a DC. The sensor automatically connects to the created MDI instance and begins collecting telemetry for detection.
This sequence aligns with Microsoft Defender for Identity deployment guidance, ensuring secure onboarding of DC1 while maintaining the principle of least privilege and meeting the business requirement to protect all domain controllers.
Final Order:
* Provide global administrator credentials #
* Create instance of Microsoft Defender for Identity #
* Provide domain administrator credentials #
* Install the sensor on DC1.

質問**: 34**
お客様は、Microsoft Copilot for Security 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。
Book1という名前のプロンプトブックを作成します。
Book1では、IncidentIDという名前の入力フィールドを含むプロンプトを作成する必要があります。
インシデントIDはどのようにフォーマットすればよいですか？
A. < IncidentID >
B. SIncidentID$

C. ##IncidentID##
D. [IncidentID]
正解: **(**正解を表示します**)**
In Copilot for Security promptbooks, inputs are referenced as placeholders wrapped in angle brackets (for example, < SENTINEL_INCIDENT_ID >). To define an input named IncidentID in a prompt, format it as < IncidentID > .

質問: **35**
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**)**
According to official Microsoft Defender for Endpoint documentation, Attack Surface Reduction (ASR) rules are specifically designed to block behaviors commonly used by malware and ransomware, such as malicious macro execution, script downloads from untrusted sources, and the abuse of Office applications to launch harmful executables or exploits.
In this scenario:
* Excel macros downloading scripts from untrusted websites are mitigated by the ASR rule:"Block Office applications from creating child processes" and "Block Office communication application from creating child processes."
* Users opening executable attachments in Outlook are covered by:"Block executable content from email and webmail."
* Outlook rules and forms exploits are addressed by:"Block Office applications from injecting code into other processes." Microsoft's Defender for Endpoint security baseline and documentation highlight that these rules "reduce the attack surface by minimizing the number of entry points an attacker can use to exploit a system." Administrators can configure them through Microsoft Intune, Group Policy, or PowerShell, and monitor their effectiveness in the Microsoft 365 Defender portal under Threat & Vulnerability Management.
Other options like Defender Antivirus (A) focus on detecting known malware after execution rather than blocking risky behaviors preemptively. Windows Defender Firewall (C) controls network traffic, not application-level threats. Adaptive application control in Azure Defender (D) is used for whitelisting applications on Azure VMs, not on Microsoft 365 endpoints.
Therefore, the correct answer is:
B: Attack surface reduction rules in Microsoft Defender for Endpoint
o365-worldwide

質問: **36**
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。

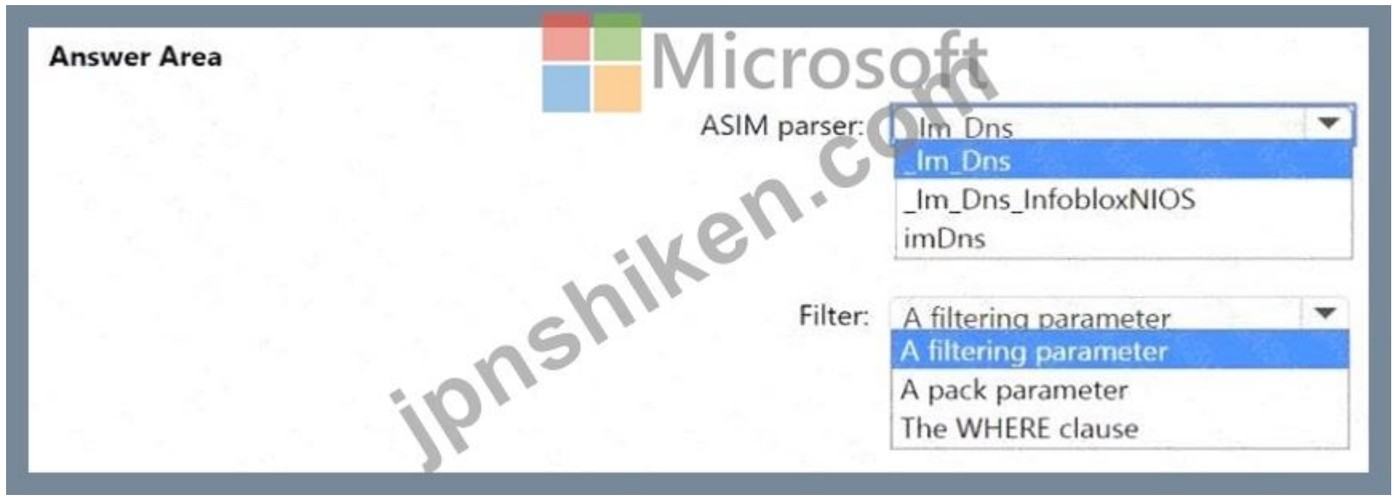
Name	Microsoft Defender status	Operating system
Device1	Onboarded	Windows
Device2	Onboarded	Windows
Device3	Onboarded	Windows
Device4	Network discovered	Other

あなたは以下の鑑識データを発見しました。
* Device1の起動中に、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。
* Device4 はポート 5555 を使用して Device! 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、processsコマンドを実行します。
* Microsoft Defender ポータルの [デバイス] から、Device1 と Device2 を隔離します。
以下の各項目について、該当する場合は 「はい」を選択してください。該当しない場合は 「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

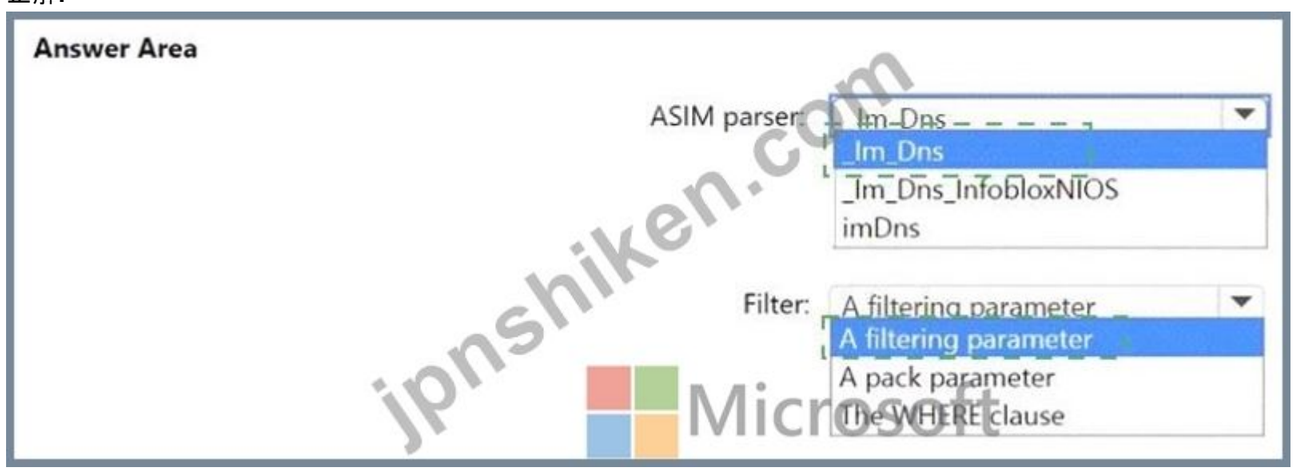
正解:

Explanation:

質問: **37**
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の要件を満たす必要があります。クエリはどのように構成すればよいでしょうか？回答するには、回答領域で適切なオプションを選択してください。注：正解ごとに1ポイントが加算されます。



正解:



Explanation:

In Microsoft Sentinel's Advanced Security Information Model (ASI M) , DNS queries are normalized through the Im_Dns parser, which unifies DNS telemetry from multiple sources (Infoblox, Windows DNS, Azure Firewall DNS proxy, etc.). Microsoft guidance states that when you need broad compatibility and want to "use built-in ASIM parsers whenever possible," you should call the generic Im_Dns() parser .

To minimize overhead , ASIM provides a pack parameter that restricts the parser to a specific content pack (vendor/source) so it won't iterate through all available source parsers under the hood. For Infoblox NIOS, you pass the Infoblox pack via the pack parameter, which limits parsing to the Infoblox implementation and reduces query cost/latency while keeping the query portable across environments.

Putting it together, the recomme nded pattern is:

Im_Dns(pack= " InfobloxNIOS ")

| where DnsResponseCodeName == " NXDOMAIN "

| summarize count()
This approach satisfies all requirements:
* Uses built-in ASIM (Im_Dns).
* Minimizes query overhead (uses pack to limit parsing to Infoblox).
* Targets NXD OMAIN responses for counting DNS request failures from Infoblox1 .

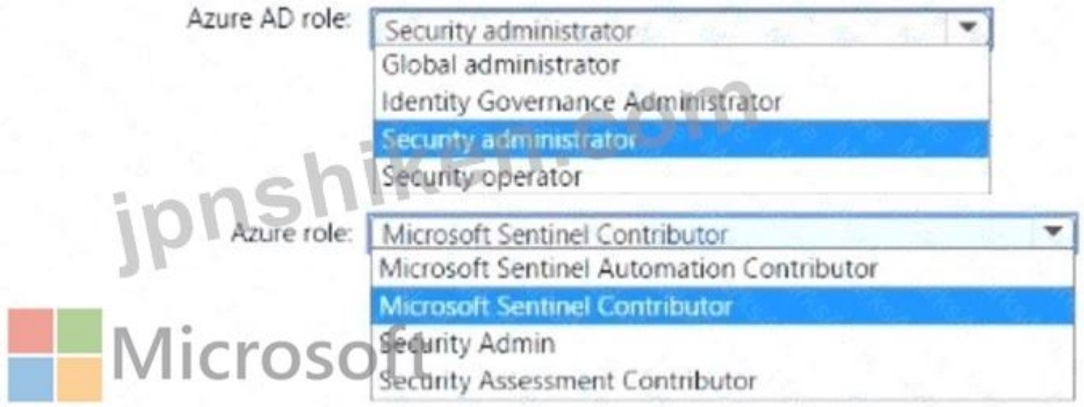
質問**: 38**
あなたは、Microsoft Copilot for Security を使用する Microsoft 365 E5 サブスクリプションをお持ちです。カスタムの Copilot for Security プラグインを作成するために、以下のコードを実行する予定です。

```
<code segment>
SkillGroups:
- Format: <target>
Skills:
```

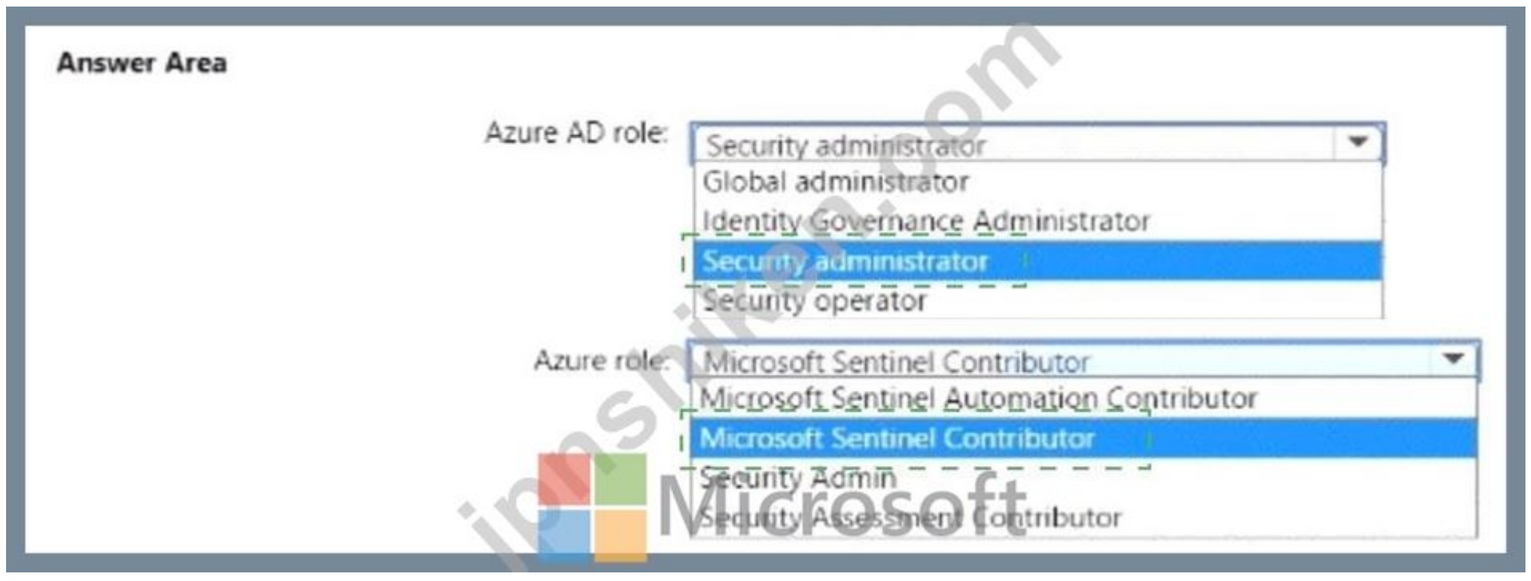
フォーマットを指定してコードを完成させる必要があります。<target>変数にはどのフォーマットを使用すればよいですか？
A. API
B. GPT
C. KQL
D. SQL
正解**: C (**コメントを発表する**)**
When authoring a custom plugin for Copilot for Security that queries security telemetry and returns structured results, the expected query/target format is Kusto Query Language (KQL) . Copilot for Security integrates with Microsoft security data platforms (Microsoft Sentinel/Log Analytics and Defender tables) where investigative and hunting queries are expressed in KQL. Official plugin examples and guidance show the plugin invoking a KQL query against a workspace or a Defender table and returning the results in the plugin response payload. KQL is the language used to interrogate event, alert, and entity tables (for example, DeviceProcessEvents, SecurityAlert, MicrosoftGraphActivityLogs) and is the supported format when a plugin's purpose is to retrieve and return telemetry to Copilot for Security. Other formats listed (API, GPT, SQL) are not the standard query language for Defender/Sentinel data: APIs are endpoints for programmatic access, GPT is a model format, and SQL is not used for Azure Monitor / Sentinel tables. Therefore when the plugin's < target > must specify the query format against security telemetry, KQL is the correct choice.

質問**: 39**
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、最小権限の原則を使用する必要があります。
「使用済み」にはどの役割を割り当てるべきでしょうか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:



Explanation:

Enabling User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel requires permissions in both Azure Active Directory (Microsoft Entra ID) and Microsoft Sentinel because UEBA integrates identity data from Azure AD to perform behavioral analytics and anomaly detection.

Here's the reasoning based on Microsoft's official documentation and the principle of least privilege:

1# # Azure AD role # Security administrator

* The Security Administrator role in Azure AD allows a user to manage security-related features , including security settings and integration of identity signals with other services like Microsoft Sentinel.
* This role has the rights necessary to grant Sentinel access to Azure AD data for UEBA without requiring broader, high-privilege roles such as Global Administrator .
* Microsoft documentation explicitly recommends the Security Administrator role to enable UEBA because Sentinel uses Azure AD identity information and risk detections for its entity behavior modeling.
2# # Azure role # Microsoft Sentinel Contributor
* Within Sentinel, the Microsoft Sentinel Contributor role allows a user to configure settings, enable features like UEBA, and manage analytic rules, workbooks, and connectors , but does not grant rights to access workspace data directly (which would be excessive).
* It's the appropriate role for managing Sentinel features while adhering to the least privilege principle.
* The Sentinel Responder role is too limited-it can handle incidents but cannot enable or configure UEBA.
# Final Answer:
* Azure AD role: Security administrator
* Azure role: Microsoft Sentinel Contributor

質問**: 40**
オンプレミスのLinuxサーバーがあり、そのサーバーはApp1という名前のバックグラウンドプロセスを実行しており、Azure Connected Machineエージェントがインストールされています。
WS1という名前のMicrosoft Sentinelワークスペースがあります。
App1に関連するメッセージを収集するために、Syslog via AMAコネクタを使用するDCR1という名前のデータ収集ルール(DCR)を設定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。
優先度レベルが ク リティカル」のメッセージのみを収集します。
収集するデータ量を最小限に抑える。
DCR1にはどの施設とログレベルを設定すべきですか？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:

When configuring the Syslog via Azure Monitor Agent (AMA) connector in Microsoft Sentinel , the Data Collection Rule (DCR) determines which Linux system logs are ingested. Syslog messages are filtered based on facility (the subsystem that generated the message) and severity level (priority) .

According to Microsoft's "Collect Syslog data sources using Azure Monitor Agent" documentation:

"Syslog facilities define which type of process generated the log (e.g., authentication, cron, daemon), and log levels define the severity (0=emerg, 1=alert, 2=crit, 3=err, etc.). To minimize data ingestion and cost, select only the facility and the highest severity level required for your investigation." In this scenario:

* You need to collect logs related to App1 , a background process (non-kernel, non-authentication, non- cron). Typically, such custom or application-level processes send logs to LOG_AUTH or LOG_DAEMON , depending on configuration. If App1 is an application that uses authentication or security features, the LOG_AUTH facility is appropriate.
* You must collect only logs with a critical priority , which corresponds to Syslog severity 2 (critical) .

In Syslog terminology, that maps to the LOG_EMERG or "emergency" level and above.

However, to ensure minimum data collection while still capturing critical events, Sentinel's best practice is to configure the Syslog DCR to collect only the specific facility associated with the application and the exact required severity level. For "critical only," LOG_EMERG is the correct choice because it ensures that only the most urgent (critical/emergency) events are ingested, reducing data volume and cost.

Final Configuration:

Setting

Correct Option

Purpose

Facility

LOG_AUTH

Collects security/authentication-related logs for App1

Log level

LOG_EMERG

Collects only critical/emergency events (priority # 0) to minimize ingestion volume In summary:

Selecting LOG_AUTH and LOG_EMERG satisfies both requirements - capturing only the highest- severity logs relevant to App1 while keeping the ingestion volume minimal, in line with Microsoft Sentinel Syslog DCR configuration guidance.

質問: **41**
Microsoft 365 Defender を使用する Microsoft 365 サブスクリプションがあります。
インシデントの影響を受けるすべてのエンティティを特定する必要があります。
Microsoft 365 Defender ポータルでどのタブを使用する必要がありますか?
A. 調査
B. デバイス
C. 証拠と対応
D. アラート
正解: **(**正解を表示します**)**
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

質問: **42**
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Log Analyticsテーブルを使用すればよいでしょうか？
A. SentwlAuoNt
B. AADRiskyUsers
C. IdentityOirectoryEvents
D. 身元情報
正解: **(**正解を表示します**)**
User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel correlates secur ity events with identity data to build behavioral baselines. UEBA enriches security signals with identity context from Azure AD, Defender for Identity, and other connected identity sources.
The IdentityInfo table in Log Analytics stores user account metadata and enrichment information , such as department, group membership, job title, and account status. This table is used to correlate events from the SecurityEvent table and others to link activity to known users and entities.
Microsoft documentation s tates:
"The IdentityInfo table contains enriched identity information from connected identity providers. It is used by UEBA to correlate with the SecurityEvent table and other identity-related logs."

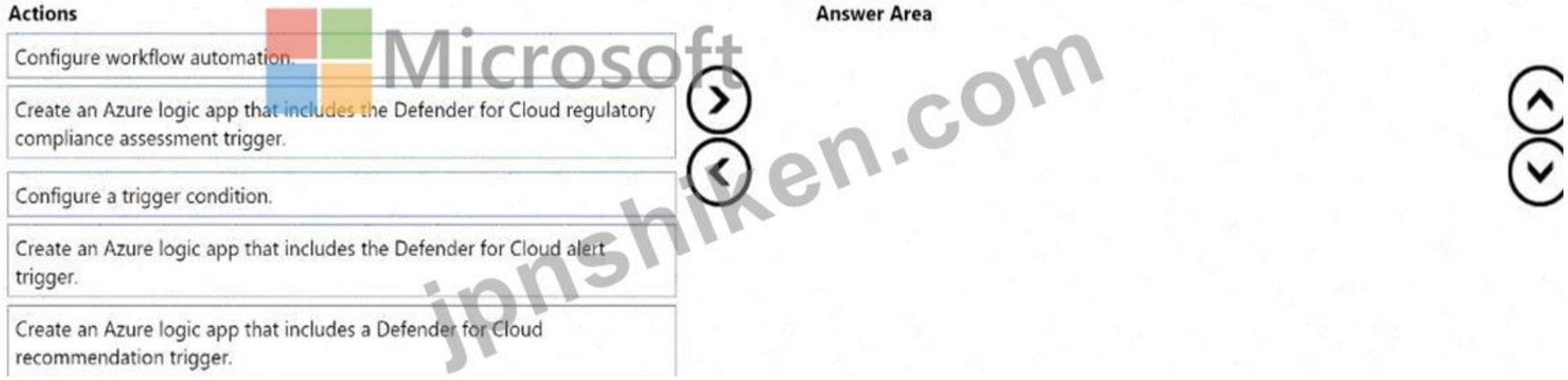
質問: **43**
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションをお持ちです。
脅威ハンティングクエリを使用することで、新たな脅威を検出できます。
Microsoft Sentinelが脅威を自動的に検出するようにする必要があります。また、管理作業を最小限に抑えるソリューションでなければなりません。
あなたはどうすべきでしょうか？
A. プレイブックを作成します。
B. ウォッチリストを作成します。
C. 分析ルールを作成します。
D. クエリをワークブックに追加します。
正解: **(**正解を表示します**)**
By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected. Reference:
https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule

質問: **44**

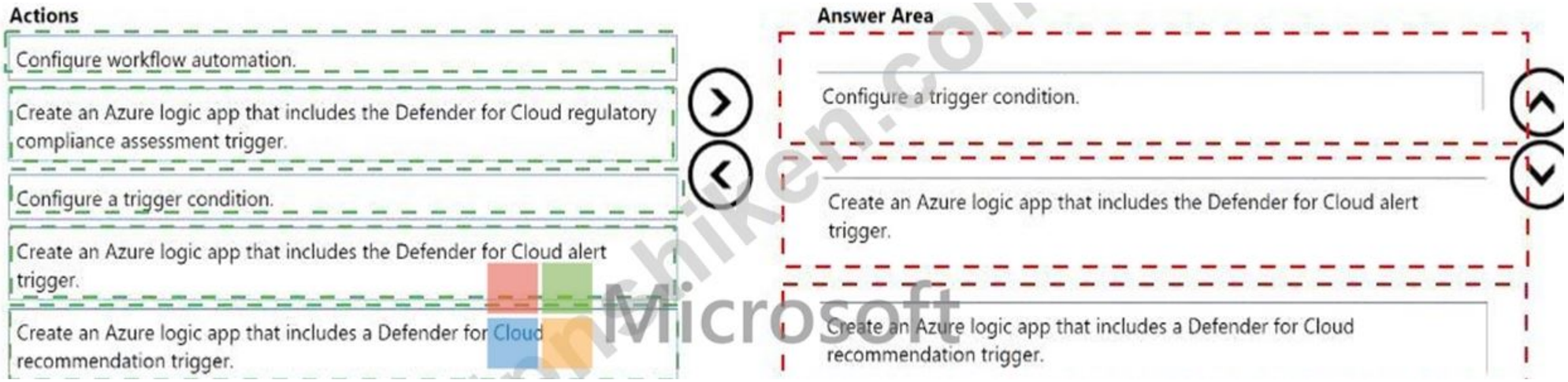
お客様は、Microsoft Defender for Cloudを使用するAzureサブスクリプションをお持ちです。

新しいMicrosoft Secure Scoreアクションが生成された際に、会社のIT部門にMicrosoft Teamsメッセージを送信するワークフローを作成する必要があります。

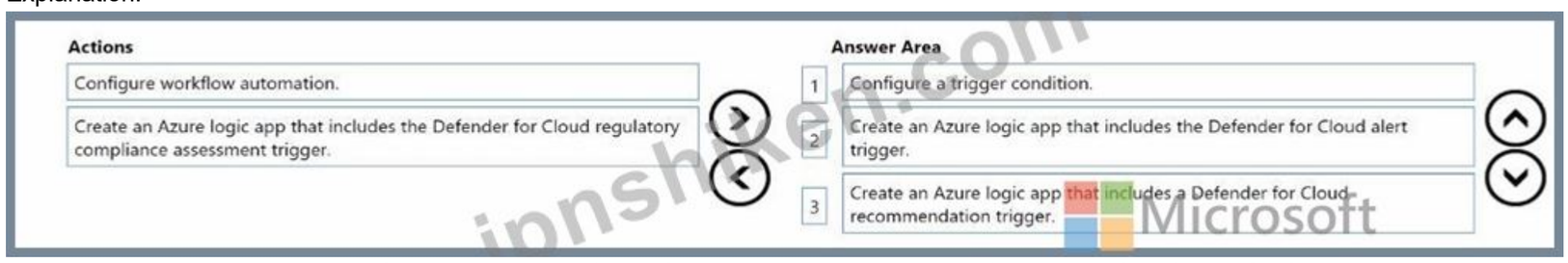
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



When you need to send a Microsoft Teams message (or perform any automated response) in Microsoft Defender for Cloud based on a new Microsoft Secure Score action , you must use workflow automation integrated with Azure Logic Apps .

Here's the correct sequence of actions, step by step:

* The Secure Score is part of Defender for Cloud's Regulatory Compliance section.
* To react to new Secure Score recommendations or actions, the Logic App must use the "When a Defender for Cloud regulatory compliance assessment is created or triggered" trigger.
* This ensures that the automation is initiated whenever a new Secure Score change occurs.
* According to Microsoft documentation:
Step 1: Create an Azure Logic App that includes the Defender for Cloud regulatory compliance assessment trigger "To automate Secure Score or compliance actions, select the 'Regulatory compliance assessment trigger' in Logic Apps. It triggers workflows when a new compliance or Secure Score recommendation is created or updated."
* Next, you configure the condition that specifies which Secure Score events should trigger the workflow.
* For example, you can set conditions such as:
* "If the assessment type = Secure Score," or
* "If compliance status = Failed."
* This filtering ensures that only relevant events (new Secure Score actions) will activate the workflow and prevent unnecessary Teams notifications.
Step 2: Configure a trigger condition
* Finally, in Defender for Cloud, you configure workflow automation to link the Logic App to the event stream.
* From the Defender for Cloud portal, navigate to Workflow automation # Add automation # Choose trigger and Logic App .
* Select the created Logic App as the target and define the scope (e.g., all subscriptions or resource groups).
* This connects Defender for Cloud to the Logic App so that when a new Secure Score event occurs, the app automatically sends the Microsoft Teams message.
Step 3: Configure workflow automation

質問: 45
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. ポリシーとルール
B. エクスプローラー
C. 脅威分析
D. 上級狩猟
正解: **(**正解を表示します**)**
In Microsoft 365 Defender , Advanced Hunting is the dedicated feature for creating and managing custom Kusto Query Language (KQL) queries used to proactively detect threats, investigate suspicious activity, and track ongoing risks across Microsoft 365 services (including Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and Defender for Office 365).
A custom tracked query is a saved hunting query that continuously assesses your environment's threat status over time. According to Microsoft documentation, you create, edit, and manage these queries under the
"Advanced Huntin g" page in the Microsoft 365 Defender portal. The tracked queries appear under the
"Custom detection rules" or "Tracked queries" tabs within this section, depending on their purpose.
Here's how it works:
* Navigate to Microsoft 365 Defender portal # Hunting # Advanced Hunting .
* Use KQL to define your custom query that identifies specific threat patterns or anomalies.
* Save it as a tracked query , allowing Microsoft 365 Defender to run it regularly and surface ongoing results in the hunting dashboard.
Other options are not correct:
* Policies & rules - used for configuration of alerting and security policies, not ad-hoc or proactive hunting.
* Explorer - provides real-time investigation of emails and threats but doesn't support custom KQL queries.

* Threat analytic s - offers intelligence-driven insights and reports but doesn't allow creating custom queries.
# Correct Answer: D. Advanced Hunting

質問: **46**
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: **D** (コメントを発表する)
Microsoft Sentinel can automatically disable scheduled analytics rules and mark them "AUTO DISABLED" when their executions repeatedly fail. A common cause is query performance issues , such as long-running queries that exceed execution time limits or hit throttling, especially with large lookback windows or inefficient joins. When a rule's query persistently times out, Sentinel halts it to protect service health and prevent unnecessary load. Other options listed don't align as primary triggers in Sentinel's auto-disable behavior: exceeding 10,000 alerts in two minutes is not the documented threshold used to auto-disable rules; generic "connectivity issues" are not specific to a single rule; permissions changes can cause failures but the well-known, tested cause that leads to the AUTO DISABLED prefix in practice is repeated timeout/failure of the query itself.

質問: **47**
Microsoft Defender for Endpoint を使用する Microsoft 365 E5 サブスクリプションをご利用の場合、マルウェア警告をトリガーしたデバイスを特定し、警告に関連する証拠を収集する必要があります。このソリューションは、収集した結果を使用して、影響を受けたデバイスの隔離を開始できることを保証する必要があります。
Microsoft 365 Defender ポータルでは何を使用すべきですか？
A. 事件
B. 調査
C. 高度な狩猟
D. 修復
正解: (正解を表示します)
In Microsoft Defender for Endpoint , an Investigation (also known as an Automated Investigation and Response - AIR) collects evidence related to alerts, analyzes device behavior, and enables response actions such as device isolation, file quarantine, or remediation .
While Incidents aggregate multiple alerts for a single attack chain, and Advanced hunting is used for custom KQL queries, Investigations are specifically designed to automate evidence collection and analysis for triggered malware alerts.
From the investigation results, analysts can then initiate isolation of affected endpoints directly in the portal.
Answer: B. Investigations

質問: **48**
Microsoft Defender for Cloud の要件を満たすには、Account! にネイティブ クラウド コネクタをデプロイする必要があります。Account! で最初に行うべきことは何ですか？
A. Defender for Cloud 用の AWS ユーザーを作成します。
B. Defender for Cloud のアクセス制御 (1AM) ロールを作成します。
C. AWS Security Hub を設定します。
D. AWS Systems Manager (SSM) エージェントをデプロイします
正解: **B (**コメントを発表する**)**
When connecting an Amazon Web Services (AWS) account to Microsoft Defender for Cloud using the native cloud connector , the very first requirement is to allow Defender for Cloud to access AWS resources securely. According to official Microsoft Defender for Cloud documentation, this is accomplished by creating an AWS Identity and Access Management (IAM) role that grants Microsoft Defender for Cloud the necessary permissions to read configuration and security data from the AWS environment.
Here's the detailed process based on Microsoft documentation:
1# # Create an IAM Role in AWS:
In the AWS console, you create an IAM role that establishes a trust relationship with Microsoft Defender for Cloud's AWS connector . The trust policy allows Azure's Defender for Cloud service principal to assume the role securely.
2# # Attach the Required Policies:
The IAM role is then granted read-only permissions by attaching the Microsoft-provided policy template.
This policy enables Defender for Cloud to assess AWS resources, collect security configuration data, and generate security recommendations.
3# # Connect the AWS Account in Defender for Cloud:
After the IAM role is in place, you return to Azure and complete the connector setup by providing the Role ARN (Amazon Resource Name). Defender for Cloud then uses this role to continuously monitor and assess the AWS environment.
Options such as creating an AWS user or configuring AWS Security Hub are subsequent integration or enhancement steps, not the first action in setting up the native connector. Deploying the SSM agent is only required for enabling Defender for Servers on AWS EC2 instances, not for the initial connector setup.
Therefore, the correct answer is B. Create an Access control (IAM) role for Defender for Cloud.

質問: **49**
お客様は、Microsoft Defender for Office 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。
配信後に検出されたものの、メールボックスから正常に削除されなかった潜在的に悪意のあるメールに関連するイベントを一覧表示する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、イベントがメール受信者のサインインイベントと関連付けられていることを保証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:

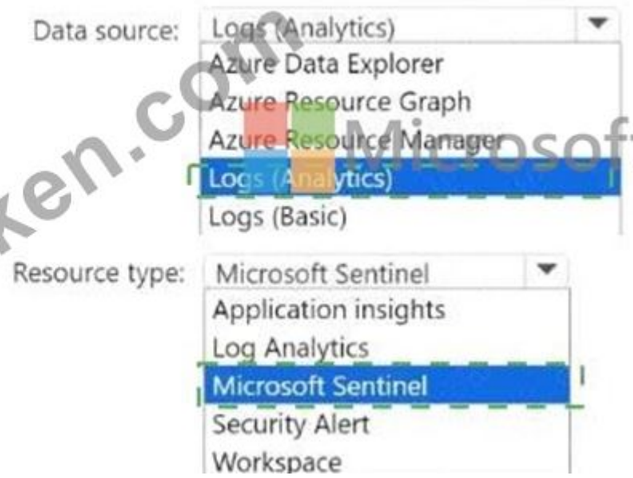
In advanced hunting, EmailPostDeliveryEvents records post-delivery actions taken on messages (e.g., Zero- hour Auto Purge - ZAP , Automated Investigation and Response). To find emails tha t were detected but not removed , filter for the post-delivery action with ActionType has " ZAP " and ActionResult == " Error " , which indicates ZAP attempted to remove the item but failed.

To correlate these mailbox events with recipient sign-ins, join to Sign inLogs . The mailbox recipient field is RecipientEmailAddress ; the corresponding identity field in sign-in data is the user principal name, exposed in normalized hunting schemas as AccountUpn . Therefore, use:
join kind=inner (...) on $left.RecipientEmailAdd ress == $right.AccountUpn A complete pattern looks like:
EmailPostDeliveryEvents
| where Timestamp > = ago(7d)
| where ActionType has " ZAP " and ActionResult == " Error "
| project ErrorTime=Timestamp, ActionType, NetworkMessageId, RecipientEmailAddress
| join kind=inner (
SigninLogs
| project AccountUpn=UserPrincipalName, AppDisplayName, Protocol, DeviceDetail) on $left.RecipientEmailAddress == $right.AccountUpn
| project ErrorTime, ActionType, NetworkMessageId, RecipientEmailAddress, AppDisplayName, Protocol, DeviceDetail This returns failed ZAP removals and the associated recipient sign-in context.

質問**: 50**
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:

Answer Area



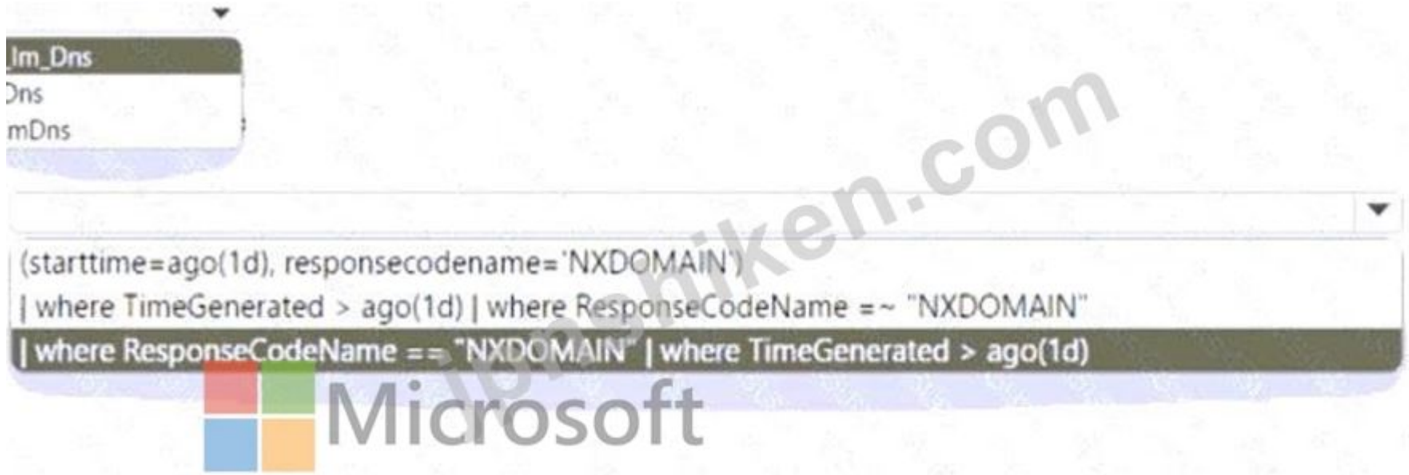
Explanation:

When you create a Microsoft Sentinel workbook that visualizes data retrieved using a Kusto Query Language (KQL) query, the workbook must use a data source that supports log analytics queries.
According to Microsoft Sentinel and Azure Monitor documentation, Logs (Analytics) is the correct data source type for querying tables stored within a Log Analytics workspace , such as the SecurityIncident table. This table is where Microsoft Sentinel stores incident data.
In the workbook configuration, the Resource type determines which service the query context applies to.
Since you are querying Microsoft Sentinel incidents (not general Azure Monitor logs or metrics), you must set the resource type to Microsoft Sentinel . This ensures that the workbook is connected to Sentinel's analytics schema and can display visualizations (charts, metrics, timelines) based on Sentinel's native data tables.
Alternative resource types such as Log Analytics or Workspace could technically access the same data, but Microsoft Sentinel documentation recommends selecting Microsoft Sentinel when the workbook is designed for security operations and incident analysis. This provides tighter integration with the SOC dashboard experience, Sentinel permissions, and security insights views.
Therefore, the correct selections are:
* Data source: Logs (Analytics)
* Resource type: Microsoft Sentinel

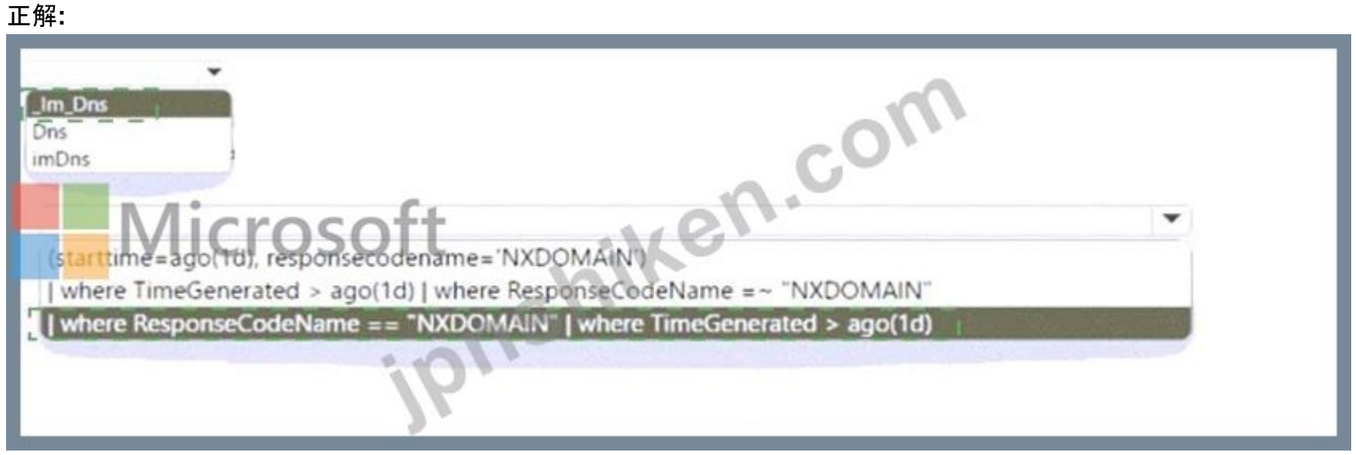
質問**: 51**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Azure セキュリティ センターを使用します。
セキュリティ センターでセキュリティ警告を受け取ります。
Security Center でアラートを解決するには、推奨事項を表示する必要があります。

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**)**
Explanation (concise): In Azure Security Center / Microsoft Defender for Cloud , the correct workflow to see recommendations for resolving a specific alert is: open Security alerts , select the alert, choose Take action , and expand Mitigate the threat to view remediation guidance. This meets the stated goal.

質問: **52**
Microsoft Sentinelワークスペースの名前はWorkspacesです。
Workspace1 を c に設定します。
DNSイベントを収集し、DNSスキーマ用の高度セキュリティ情報モデル(ASIM)統合パーサーを展開します。
ASIM DNSスキーマに対してクエリを実行し、過去24時間以内に応答コードが「NXDOMAIN」で、送信元IPアドレスごとに15分間隔で集計されたすべてのDNSイベントを一覧表示する必要があります。このソリューションは、クエリのパフォーマンスを最大限に高める必要があります。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。注：正解ごとに1ポイントが加算されます。



正解:



Explanation:

When you deploy the ASIM unifying parser for DNS , you should query the normalized schema via the function imDns() (ASIM convention: im < Domain >). To maximize performance , pass filtering arguments directly to the parser so the function prunes data early at source, ra ther than piping a large dataset into subsequent where filters. ASIM DNS supports parameters such as starttime , endtime , and responsecodename (for example, NXDOMAIN). Therefore, using imDns(starttime=ago(1d), responsecodename= ' NXDOMAIN
') limits ingestion t o the last 24 hours and only events whose ResponseCodeName equals NXDOMAIN .
Once normalized rows are returned, use summarize with bin() to aggregate efficiently. The ASIM DNS schema exposes the client address as SrcIpAddr ; grouping by this field and bin(TimeGenerated, 15m) produces per-source-IP counts in 15-minute buckets. The final query:
imDns(starttime=ago(1d), responsecodename= ' NXDOMAIN ')
| summarize count() by SrcIpAddr, bin(TimeGenerated, 15m)
meets all requirements: it lists all DNS events with NXDOMAIN in the last 24 hours and aggregates them by source IP in 15-minute intervals , using ASIM's parameterized parser to achieve optimal performance.

質問: **53**
技術要件を満たすためには、ログイン失敗に関するクエリを完了する必要があります。
WHERE句を完成させるための列名はどこで確認できますか？
A. Azure Security Center のセキュリティ警告
B. Azureのアクティビティログ
C. Azure Advisor
D. Log Analyticsワークスペースのクエリウィンドウ
正解: **(**正解を表示します**)**
To complete the KQL query against the BehaviorAnalytics t able, you need to know the exact column name (for example, the Boolean field that flags a new or first-time country for the sign-in). Microsoft's standard method to discover table schemas and column names is the Logs (Log Analytics) query window . In this p ane, the left-hand Schema browser lists all connected tables and, when expanded, shows every column name and data type . Selecting a table (e.g., BehaviorAnalytics) reveals its fields, and the editor provides IntelliSense/autocomplete for columns as you typ e your KQL, making it straightforward to complete a clause like | where < ColumnName > == true .
Security alerts in Azure Security Center (Defender for Cloud), the Azure Activity log, and Azure Advisor do not expose the per-table column schema needed to build KQL filters. Security Center surfaces alerts and recommendations; the Activity log records control-plane operations; and Advisor provides optimization guidance-none of these replace the Logs experience for exploring data schemas.
Therefore, to accurately identify and verify the column required in the where clause for failed sign-ins from a first-time country, you should use the Log Analytics workspace query window , consult the Schema pane for the BehaviorAnalytics table, and leverage the editor's autocompl ete to insert the correct column name.
Topic 2, Litware inc.
Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided i n the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study

To display th e first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing envir onment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Litware Inc. is a renewable company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment

Identity Environment

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litw are has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

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

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

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

Current problems

Cloud App Security frequently ge nerates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by us ing Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

* The principle of least privilege must be used whenever possible.
* Costs must be minimized, as long as all other requirements are met.
* Logs collected by Log Analytics must provide a full audit trail of user activities.
* All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are store d on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.

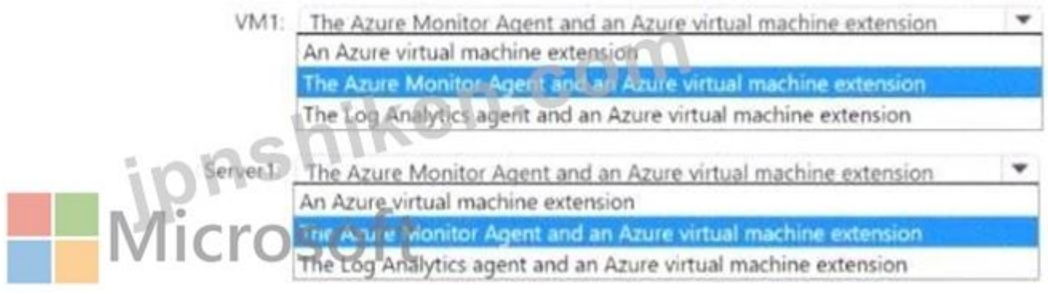
Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using M icrosoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

質問: 54
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	On-boarded to Azure Arc 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。
導入と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。
Answer Area



正解:

Answer Area

Explanation:

For SQL Server on Azure VMs (VM1) , Defender for Cloud's Advanced Threat Protection and Vulnerability Assessment for SQL "on machines" are enabled by registering the instance as a SQL virtual machine using the SQL IaaS Agent extension . This single Azure VM extension onboards the SQL workload, exposes SQL VM resource management, and lights up Defender for SQL (ATP + VA) with minimal admin effort-no separate agents are required on Azure VMs beyond this extension for these features.

For on-premises/Arc servers (Server1) , the machine is already Arc-enabled . To protect SQL instances with Defender for Cloud and to surface vulnerabi lity assessment and threat protection signals, you deploy the Azure Arc SQL Server extension (delivered as an Arc "virtual machine extension") to register the instance with Azure. In addition, Arc scenarios use the Azure Monitor Agent (AMA) for data collec tion and security signal ingestion in Defender for Cloud (the legacy Log Analytics agent is not recommended). This combination satisfies ATP/VA requirements while keeping operations simple and consistent with current agent guidance.

Therefore:

* VM1: only th e Azure VM extension (SQL IaaS Agent extension).
* Server1: AMA + an Azure (Arc) extension (Arc SQL Server extension).

質問**: 55**

Microsoft Defender for Office 365 に安全な添付ファイル ポリシーを実装します。

ユーザーは、添付ファイルを含む電子メール メッセージの受信に予想よりも時間がかかると報告しています。

セキュリティを損なうことなく、添付ファイルを含むメッセージを配信するのにかかる時間を短縮する必要があります。添付ファイルでマルウェアをスキャンし、マルウェアを含むメッセージをブロックする必要があります。

安全な添付ファイルのポリシーでは何を構成する必要がありますか?

A. 動的配信

B. 置換

C. リダイレクトをブロックして有効にする

D. リダイレクトを監視して有効にする

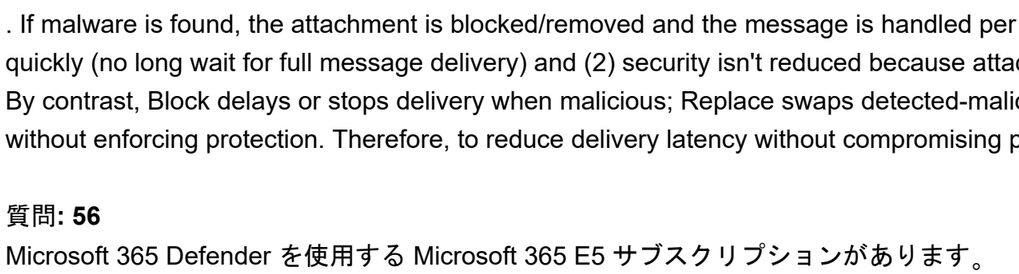
正解**: (**正解を表示します**)**

In Microsoft Defender for Office 365 Safe Attachments, Dynamic Delivery is specifically designed to shorten perceived delivery time while keeping full detonation scanning in place. Microsoft explains that with Dynamic Delivery, the service "delivers the message body right away and replaces attachments with a placeholder while scanning"; once the sandbox verdict is clean, the original file is reinserted automatically

. If malware is found, the attachment is blocked/removed and the message is handled per policy (for example, quarantined). This option meets both requirements in the question: (1) users get messages quickly (no long wait for full message delivery) and (2) security isn't reduced because attachments are still detonated before users can open them.
By contrast, Block delays or stops delivery when malicious; Replace swaps detected-malicious attachments with a .txt summary but doesn't reduce the initial delivery time for clean items; Monitor only logs without enforcing protection. Therefore, to reduce delivery latency without compromising protection and still block malware, configure Dynamic Delivery in your Safe Attachments policy.

質問: **56**
Microsoft 365 Defender を使用する Microsoft 365 E5 サブスクリプションがあります。
Microsoft が発見した新しい攻撃手法を確認し、サブスクリプション内の脆弱なリソースを特定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。Microsoft 365 Defender ポータルではどのブレードを使用する必要がありますか?
A. 高度なハンティング
B. 脅威分析
C. インシデントとアラート
D. 学習ハブ
正解: **(正解を表示します)**
To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help yo u identify risks and prioritize threats in your environment.
Reference: https://docs.microsoft.com/en-us /microsoft-365/security/mtp/microsoft-365-defender-threat- analytics

質問: **57**
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)を有効にできるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1にはどの役割を割り当てるべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:

Explanation:
Microsoft Entra role: Security Administrator

Role for WS1: Microsoft Sentinel Contributor
To enable User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel , a user must have permission to configure data connectors that access Microsoft Entra ID (Azure AD) identity data and to manage Sentinel settings for the workspace.
This requires roles in two scopes :
1# # Microsoft Entra ID (directory) level - for identity data access.
2# # Sentinel workspace level - for Sentinel feature management.
Step 1: Microsoft Entra (Azure AD) Role # Security Administrator According to Microsoft documentation, enabling UEBA requires connecting Microsoft Sentinel to Microsoft Entra ID to import user and identity behavior data.
The Security Administrator role grants the necessary read permissions to user and sign-in data while still adhering to the principle of least privilege .
* The Global Administrator role would also work but provides excessive privileges beyond what's required for UEBA configuration.
* The Security Operator role is limited to viewing alerts and cannot configure Sentinel connectors.
Hence, Security Administrator is the correct least-privilege directory role.
Step 2: Role for WS1 (Sentinel Workspace) # Microsoft Sentinel Contributor To manage Sentinel configuration and enable features such as UEBA , data connectors , and analytics rules , the Microsoft Sentinel Contributor role is required at the workspace level.
* The Sentinel Contributor role allows enabling/disabling features, managing playbooks, and configuring connectors.
* The Sentinel Automation Contributor role is only for playbook automation permissions.
* The basic Contributor role can manage Azure resources but doesn't grant Sentinel-specific privileges.
# Final answer:
* Microsoft Entra role: Security Administrator
* Role for WS1: Microsoft Sentinel Contributor

質問: 58
Microsoft Sentinelワークスペースをお持ちです。
Microsoft Defenderコネクタによって生成されたインシデントを一時的に抑制するには、Fusion Analyticsルールを構成する必要があります。このソリューションは、以下の要件を満たす必要があります。
多段階攻撃の検出能力への影響を最小限に抑える。
管理業務の手間を最小限に抑える。
ルールはどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

Answer Area

Explanation:

Answer Area

The Fusion analytics rule in Microsoft Sentinel automatically correlates alerts from multiple sources (including Microsoft Defender connectors) to detect multistage attacks . Because Fusion runs continuously and cannot be disabled without losing multi-stage detection, the best practice for temporarily suppressing incidents from a specific connector (like Microsoft Defender) is to use automation rules , not by disabling the Fusion rule itself.

An automation rule can be configured to trigger on specific conditions (such as "When incident is updated" or "When incident is created") and then perform an action like running a playbook that applies suppression logic.

Here's the reasoning:

* Trigger:
* Setting the trigger to "When incident is updated" ensures that the rule evaluates changes to existing incidents-such as enrichment or tagging from Fusion-and provides finer control over suppression, minimizing impact on the Fusion detection pipeline.
* Using "When incident is created" could interfere with Fusion's initial detection process.
* Action:
* The appropriate action is "Run playbook" , which allows automated handling (for example, tagging or closing certain incidents from a specific connector). This requires minimal administrative effort and avoids turning off the Fusion rule.

This configuration ensures that Fusion continues to detect multistage attacks (so detection isn't impacted) while automation handles temporary suppression for specific connectors efficiently.

質問: **59**

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. 資産ルール

C. ハニートークンエンティティタグ

D. 機密性の高いエンティティタグ
正解**: (**正解を表示します**)**
In Microsoft Defender XDR , the attack surface map visually prioritizes assets that are tagged as critical to your organization's operations. According to Microsoft's documentation:
"Critical asset rul es help ensure high-value or sensitive resources are highlighted on the attack surface map for monitoring and correlation in incidents." To have DB1 (a database server) appear on the attack surface map, it must be designated as a critical asset .
When you c onfigure a critical asset rule , Defender XDR automatically classifies and surfaces that system on the map, enabling enhanced monitoring, prioritization, and contextual correlation in security incidents.
Other options do not achieve this:
* Asset rule : general classification, not used for attack surface prioritization.
* Honeytoken entity tag : marks decoy assets for threat detection.
* Sensitive entity tag : used for sensitivity context in data or user-based scenarios.
# Correct answer: A. a critical asset rule

質問**: 60**
お客様は、Microsoft Defender 36S 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、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。
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
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

union
- join kind=full outer
- join kind=inner
- union

IdentityLogonEvents
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents

正解:

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

union dropdown: join kind=full outer / join kind=inner / union

IdentityLogonEvents dropdown: IdentityInfo / IdentityLogonEvents / IdentityQueryEvents

Explanation:

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

jpnshiken.com

Microsoft

To combine sign-in attempts from endpoints and on-premises AD DS domain controllers in Microsoft 365 Defender advanced hunting, you should query the tables that record those events and union them.

DeviceLogonEvent s contains interactive and network logon activity collected from devices onboarded to Microsoft Defender for Endpoint , while IdentityLogonEvents contains sign-in activity observed by Microsoft Defender for Identity sensors on domain controllers . Using unio n appends the rows from both sources into a single result set while preserving columns such as Timestamp , AccountDomain , AccountName , AccountUpn , and AccountSid . This is preferable to a join because the goal is to list sign-in attempts (not correlate rows between tables). Applying take 100 to each table segment ensures you're pulling the 100 most recent entries from each source before unioning, then you can reorder and sort by Timestamp to review the consolidated timeline.
Therefore, to meet the requirement - identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers -complete the KQL with union and IdentityLogonEvents .

質問: **61**
Azure Sentinel でハンティング クエリを作成します。
ハンティング クエリでクエリの一致が検出されたら、すぐに Azure portal で通知を受け取る必要があります。ソリューションは労力を最小限に抑える必要があります。
何を使えばいいのでしょうか？
A. プレイブック
B. ノートブック
C. ライブストリーム
D. ブックマーク
正解: **C (**コメントを発表する**)**
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

質問: **62**
あなたはMicrosoft 365 B5サブスクリプションをお持ちです。統合監査ログを照会するPowerShellスクリプトをお持ちです。
サーバー側のページング処理により、クエリの結果が最初のページしか返されないことがわかりました。すべての結果を取得するには、どのプロパティをクエリすればよいでしょうか？
A. @odata.nextlink
B. @odata.deltaLink
C. @odata.context
D. @odata.count
正解: **(**正解を表示します**)**
When querying the Microsoft 365 Unified Audit Log (via Graph API or PowerShell), results are paginated for performance. The property @odata.nextLink provides the URL for the next page of results. You must keep querying this link until it no longer appears to retrieve all entries.
* @odata.deltaLink is used for incremental changes (next query after initial).
* @odata.context describes the response metadata.
* @odata.count indicates record count only. Thus, to retrieve all paged results , use @odata.nextLink .
# Answer: A. @odata.nextLink

質問: **63**

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

Document」という名前の添付ファイルを含むすべてのメールを返す検索クエリを作成する必要があります。

PDFファイル。クエリは以下の要件を満たす必要があります。

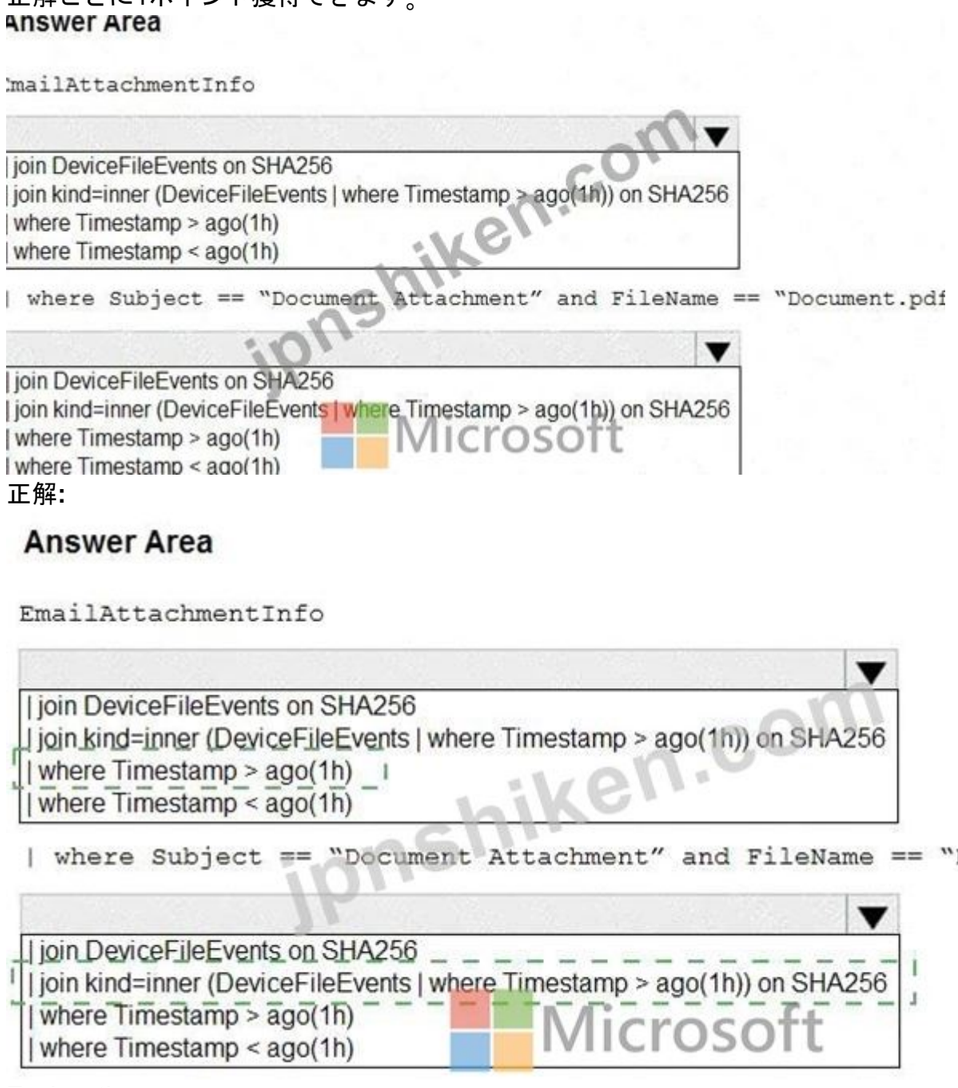
* 過去1時間以内に送信されたメールのみを表示します。

* クエリのパフォーマンスを最適化します。

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

正解ごとに1ポイント獲得できます。

Answer Area



正解:

Answer Area

Explanation:

For hunting in Microsoft 365 Defender , email at tachment metadata is in EmailAttachmentInfo (fields include Timestamp , FileName , SHA256 , NetworkMessageId , etc.). To return every email that contains a specific attachment and optimize performance , apply time filters as early as possible and avoid unnecess ary joins. Early filtering reduces the dataset to scan and speeds execution.
A performant query that meets "only last hour" and the attachment name requirement is:
EmailAttachmentInfo
| where Timestamp > ago(1h) // filter early for perf ormance
| where Subject == " Document Attachment " and FileName == " Document.pdf "
| where Timestamp > ago(1h) // (idempotent second constraint; harmless) Using joins (e.g., to DeviceFileEvents on SHA256) is not required to answer the question and would add overhead. The key is to filter on Timestamp and FileName within EmailAttachmentInfo , ensuring only emails from the last hour with Document.pdf are returned while keeping the query efficient.

質問**: 64**
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**)**
Comprehensive and Detailed Explanation with all Microsoft Security Operations (SecOps) documents :
=
To monitor Linux virtual machines in AWS using Azure Defender (Microsoft Defender for Cloud) , you must onboard those VMs into Azure's management plane. The recommended and supported approach is via Azure Arc .
Azure Arc enables Azure Defender to extend its security monitoring and policies to non-Azure machines (including AWS and on-premises). Once onboarded through Azure Arc, the Log Analytics agent (MMA /AMA) can be automatically provisioned, allowing Defender for Cloud to collect and analyze security data.
Microsoft documentation states:
"To monitor machines outside Azure (on-premises or in other clouds like AWS or GCP), onboard them to Azure using Azure Arc. Azure Defender will then auto-provision the required agent and begin monitoring." Thus, enabling Azure Arc and onboarding the AWS VMs meets the goal .
Correct answer: A. Yes

質問**: 65**
Microsoft Sentinelの要件を満たすために、ハンティングクエリを実行できることを確認する必要があります。どのようなタイプのワークスペースを作成すればよいでしょうか？

A. Azure Synapse AnarytKS
B. AzureDalabricks
C. Azure Machine Learning
D. LogAnalytics
正解: **(**正解を表示します**)**
Microsoft Sentinel is built on top of Azure Monitor Log Analytics . All Sentinel data - including security alerts, incidents, and telemetry from connected sources - is stored and queried through a Log Analytics workspace . Sentinel's hunting feature uses Kusto Query Language (KQL) , which runs directly against the Log Analytics workspace data.
Official Sentinel documentation specifies:
"Microsoft Sentinel uses an Azure Monitor Log Analytics workspace as its foundation. All data collected by Sentinel is stored in that workspace, and hunting queries run on this data." Other workspace types such as Azure Synapse , Azure Databricks , or Azure Machine Learning are for analytics, data science, and modeling - not security log collection or KQL-based hunting.
Therefore, to run hunting queries in Microsoft Sentinel, you must create a Log Analytics workspace.

質問: **66**
Microsoft Sentinelワークスペースの名前はWorkspacesです。
組み込みの統合 ASIM パーサーから、ソース固有の組み込み 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. ワークブック
B. ハンティングクエリ
C. ウォッチリスト
D. 解析規則
正解: **(**正解を表示します**)**
To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic r ule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used. Reference: https://docs.micros oft.com/en-us/azure/sentinel/analytics-create-analytic-rule

質問: **67**
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**)**
In Microsoft Defender for Cloud (previously Azure Security Center and Azure Defender), email notifications for security alerts are configured under the "Pricing & settings" section of the workspace or subscription settings. According to Microsoft documentation, each subscription connected to Defender for Cloud has a "Pricing & settings" page that allows administrators to manage configurations such as Defender plan activation, data collection settings, and email notifications for security alerts.
To enable the SOC team to receive alert notifications, you navigate to Microsoft Defender for Cloud # Environment settings # [Select Subscription] # Pricing & settings # Email notifications. There, you can specify:

* The email addresses (up to 200) that will receive alerts.
* Whether to send notifications for high-severity alerts only or for all alerts.
* Whether to send to subscription owners, contributors, or specific emails.
This configuration ensures that alert emails are automatically sent whenever Defender for Cloud generates new security alerts, allowing the Security Operations team to stay informed without manual monitoring.
The other options are incorrect because:
* Security solutions is for integrating third-party or partner security products.
* Security policy defines compliance and assessment standards.
* Security alerts shows existing alerts but does not control notification settings.
* Azure Defender is the protection plan; it doesn't control notification preferences.
Therefore, the correct answer is C. Pricing & settings.

質問: 68
お客様のオンプレミスネットワークにはHyper-Vクラスターが存在します。このクラスターには、次の表に示す仮想マシンが含まれています。

Name	Operating system	Azure Connected Machine agent	Azure Monitoring Agent
Server1	Windows Server 2019	Not installed	Installed
Server2	Windows Server 2016	Installed	Not installed
Server3	Linux Ubuntu 20.04	Not installed	Installed

SW1という名前のMicrosoft Sentinelワークスペースがあります。
データ収集ルール(OCR)には、以下の設定があります。
* 名前: DCR1
* 行き先: SW1
* プラットフォームの種類: すべて
* データ収集エンドポイント: なし
* データソース :Windowsイベントログ、Linux syslog
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
Server1 can be added to DCR1 as a resource and all the Windows event logs can be gathered.	○	○
Server2 can be added to DCR1 as a resource and specific Windows event log events can be gathered.	○	○
Server3 can be added to DCR1 as a resource and all the Linux syslog data can be gathered.	○	○

正解:

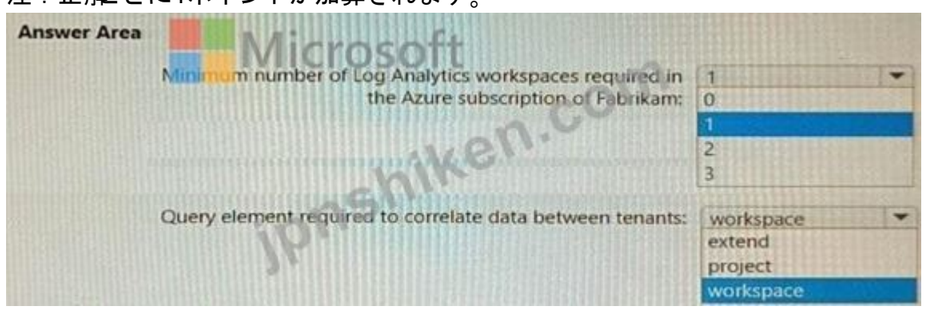
Explanation:
No
Yes
No

質問: **69**
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. 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。
B. Microsoft 365 アプリ コネクタを作成します。
C. Microsoft 365 Defender への自動リダイレクトを有効にします。
D. Azure アプリ コネクタを作成します。
正解: **(**正解を表示します**)**
In Microsoft Defender for Cloud Apps (MCAS) , Cloud Discovery collects traffic logs to identify shadow IT usage and cloud app activiti es. To enrich this discovery data and map the usernames in traffic logs to actual Microsoft Entra ID (Azure AD) users, Defender for Cloud Apps must correlate the username with the user's User Principal Name (UPN) .
According to Microsoft Defender for Cloud Apps documentation, this correlation happens automatically when you connect Microsoft 365 (formerly Office 365) through a Microsoft 365 app connector .
The connector integrates MCAS with Microsoft 365, allowing it to:
* Normalize usernames from discovery logs to match UPNs.
* Provide enriched identity details and activities across Microsoft 365 apps.
* Enable cross-app investigation, alert correlation, and conditional access governance.
Other options explained:
* Conditional Access App Control - Used for real-time s ession control, not Cloud Discovery enrichment.
* Enable automatic redirection to Microsoft 365 Defender - Used for portal integration, not data enrichment.
* Azure app connector - Used to connect third-party or Azure-hosted applications, not for UPN enrichmen t.
# Therefore, to enrich Cloud Discovery data with UPN mapping, you must create a Microsoft 365 app connector .

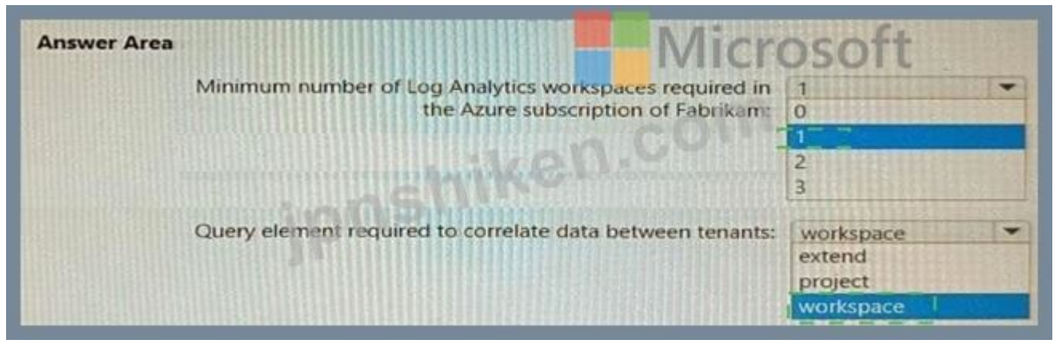
質問: **70**
Microsoft Defender for Cloud を使用し、Windows Server を実行する 100 台の仮想マシンを含む Azure サブスクリプションがあります。
仮想マシンからイベント データを収集するには、Defender for Cloud を構成する必要があります。ソリューションでは、管理の労力とコストを最小限に抑える必要があります。
どの 2 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。

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: **A,E (**コメントを発表する**)**
Microsoft Defender for Cloud collects security-related event data from virtual machines (VMs) by connecting them to a Log Analytics workspace. To minimize both administrative overhead and cost, the most efficient configuration invol ves automatic provisioning and setting an appropriate data collection level .
* Automatic Provisioning (Option E): According to Microsoft Defender for Cloud documentation, enabling automatic provisioning ensures that the Log Analytics agent (also known as the Defender for Cloud agent) is automatically installed and configured on all existing and new Azure virtual machines.
This eliminates the need for manual agent deployment, significantly reducing administrative effort.
* Data Collection Level - Common (Option A): Defender for Cloud allows configuration of event collection levels - None , Common , and All Events .
* Common collects essential security events needed for threat detection, such as logon failures, account lockouts, and other critical activities, thereby r educing storage and processing costs.
* All Events collects all Windows security logs, increasing data volume and cost without necessarily improving detection for most environments.
By combining automatic provisioning with the "Common" event level, you ensur e coverage for Defender for Cloud's analytics with minimal manual configuration and optimized costs.
Therefore, the correct and verified answer is:
A. Set data collection level to Common
E. Enable automatic provisioning for the virtual machines

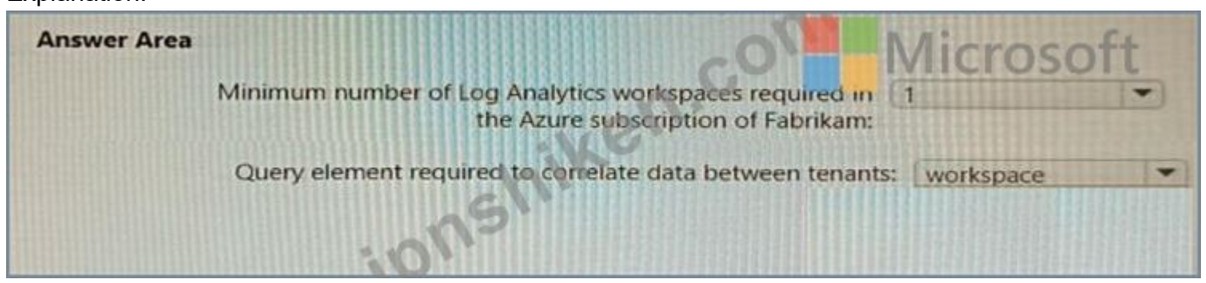
質問: 71
技術要件を満たすためには、ContosoとFabrikam向けにMicrosoft Sentinelクエリを実装する必要があります。
解答には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



In Microsoft Sentinel, each workspac e acts as a logical container for security data and analytics. When integrating Sentinel across organizations or environments-such as between Contoso and Fabrikam - each Azure subscription needs at least one Log Analytics workspace that Sentinel can attach t o. This workspace becomes the data repository for logs and analytics rules.

Therefore, Fabrikam requires a minimum of one Log Analytics workspace to onboard Microsoft Sentinel and begin collecting and analyzing data. Multiple workspaces may be used for isolation or region-specific requirements, but one is sufficient for a functional deployment.

To query and correlate data between multiple workspaces or tenants , Sentinel uses the workspace() KQL function. This function allows cross-workspace queries, lett ing you pull data from different Sentinel instances for investigation or threat correlation. For example:

union workspace(" FabrikamWorkspace ").SecurityEvent, workspace(" ContosoWorkspace ").

SecurityEvent

| summarize count() by Account

This KQL syntax enables cross-tenant or cross-subscription correlation when Defender or Sentinel workspaces are connected through proper permissions (e.g., Azure Lighthouse or cross-tenant data access).

Final Answers:

* Minimum number of Log Analytics workspaces: 1

* Query element required to correlate data between tenants: workspace

質問**: 72**

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?

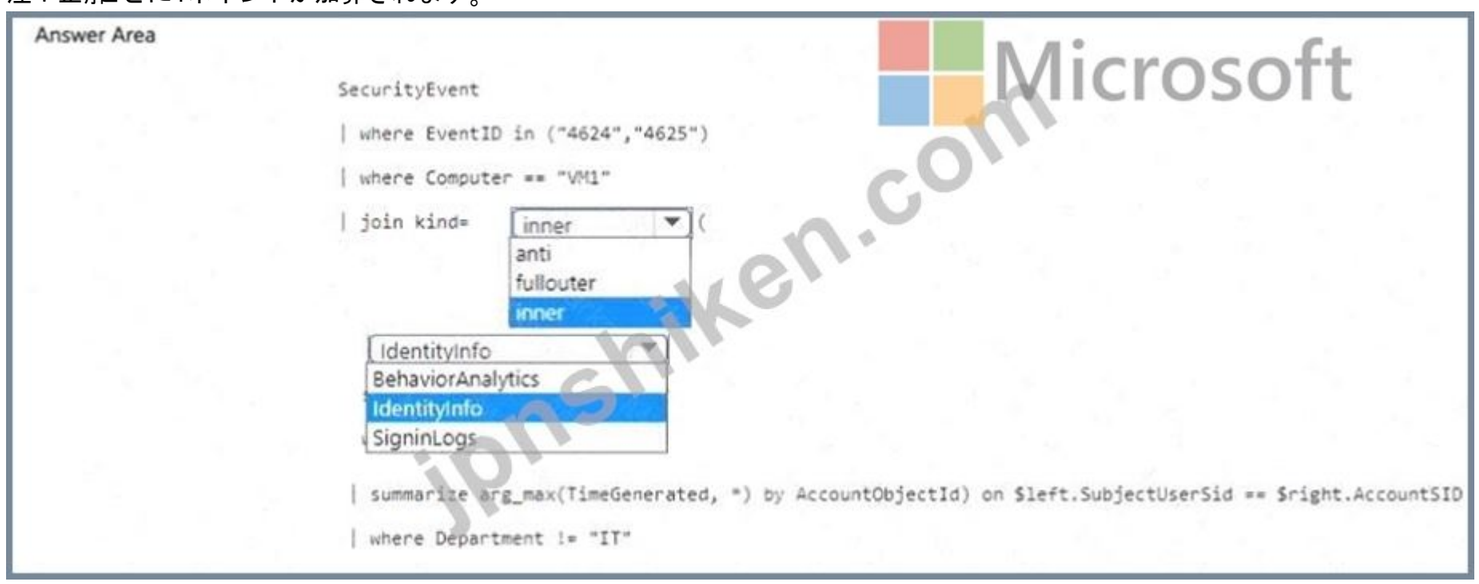
A. はい
B. いいえ
正解: **(**正解を表示します**)**
In Azure Security Center (now part of Microsoft Defender for Cloud), when you receive a security alert, you can investigate it to understand the cause, impact, and resolution recommendations.
The workflow described in the question aligns precisely with Microsoft's documented process for investigating alerts.
From the Security alerts page:
* You select the specific alert to open the alert details pane.
* Choose Take Action to view remediation options and recommended next steps.
* Expand the Prevent future attacks section - this section provides recommendations and hardening guidance directly related to the alert to help prevent similar issues from occurring again.
This section is specifically mentioned in Microsoft Defender for Cloud documentation:
"In the alert details page, select Take Action to view the remediation steps. Under Prevent future attacks , Defender for Cloud lists relevant security recommendations and actions that can mitigate or prevent the threat." Therefore, this solution meets the goal because selecting Take Action and expanding Prevent future attacks directly exposes the recommended remediation steps associated with that alert.
Answer: A. Yes

質問**: 73**
Azure Sentinel データを視覚化し、サードパーティのデータ ソースを使用してデータを強化し、侵害の兆候 (IoC) 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 Sentinel のノートブック
B. Microsoft Cloud App Security
C. Azure モニター
D. Azure Sentinel でのクエリのハンティング
正解: **(**正解を表示します**)**
According to Microsoft Sentinel documentation, notebooks integrate with Azure Machine Learning and Jupyter to allow advanced data visualization, enrichment, and correlation with third-party data sources.
Notebooks are used by security analysts and threat hunters to perform deep investigations by combining Sentinel data (such as logs, alerts, and incidents) with external threat intelligence feeds, indicators of compromise (IoCs), and custom datasets.
Microsoft describes notebooks as:
"A powerful tool built on Jupyter and Azure Machine Learning that allows you to use Python code to enrich Microsoft Sentinel data with external data sources, visualize data, and identify patterns and IoCs."
They allow analysts to query, visualize, and correlate data interactively, going beyond the built-in dashboards and KQL-based analytics.
Thus, to visualize Sentinel data and enrich it with third-party IoC data, Notebooks in Azure Sentinel is the correct solution

質問**: 74**
あなたは、User1とUser2という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います。Copilot for Securityポータルから、User1はセッションを開始し、次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1のみ
B. プロンプト1とプロンプト2のみ

C. プロンプト3のみ
D. プロンプト1とプロンプト3のみ
E. プロンプト1、プロンプト2、およびプロンプト3
正解: **D (**コメントを発表する**)**
In Microsoft Copilot for Security , when a user shares a Copilot session with another user, access control to the data sources (plugins) used within that session follows the principle of least privilege - meaning shared session visibility is determined by the viewer's own permissions to the underlying data sources.
According to Microsoft documentation:
"When you share a Copilot for Security session, other participants can see results only for data and plugins they are licensed for and authorized to access." In this scenario:
* Prompt1 and Prompt3 use the Entra plugin .
* Both User1 and User2 have access to Entra ID # therefore, User2 can view these results.
* Prompt2 uses the Intune plugin , but User2 does NOT have Intune access # thus, User2 cannot view the results of Prompt2 in the shared session.
# Correct Answer: D. Prompt1 and Prompt3 only

質問: **75**
お客様は、以下のリソースを含む Azure サブスクリプションをお持ちです。
* Windows Serverを実行するVM1という名前の仮想マシン
* 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 Sentinel1 という名前の Microsoft Sentinel ワークスペース。VM1 へのサインイン試行を追跡する Rule1 という名前のスケジュール済みクエリ ルールがあります。
社内のIT部門以外のユーザーがVM1にサインインしたことを検出するために、ルール1を更新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。
* UEBAの結果を活用する。
クエリのパフォーマンスを最大化する。
偽陽性の数を最小限に抑える。
ルール定義はどのように完成させるべきですか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:

Explanation:

To detect sign-ins to VM1 by users outside the IT department while leveraging UEBA, you should enrich Windows security events with identity attributes from UEBA's enrichment tables . In Microsoft Sentinel, UEBA writes organizational attributes (e.g., Department, Title, AAD object IDs/SIDs) to the IdentityInfo table. Joining SecurityEvent (Event IDs 4 624/4625) with IdentityInfo on the user SID lets you filter with where Department != " IT " -meeting the requirement to utilize UEBA results .

For performance and fewer false positives, use join kind=inner . An inner join only returns rows where the user in Sec urityEvent has a corresponding identity record in IdentityInfo , avoiding unmatched and potentially noisy events. Options like fullouter would introduce non-matching rows (increasing noise), and anti would return only unmatched rows (the opposite of what's needed).

BehaviorAnalytics contains anomaly scores/events rather than static attributes like department, and SigninLogs is raw AAD sign-in telemetry (not the UEBA-enriched identity inventory needed for department filtering). Therefore, IdentityInfo is the correct enrichment source.

Thus, to satisfy use UEBA, maximize performance, and minimize false positives : join kind=inner with IdentityInfo and then filter Department != " IT " .

質問: **76**

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。

あなたは、Windows Server 2022 を実行し、Amazon Web Services (AWS) でホストされている Server! という名前の仮想マシンを持っています。

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 Arc エージェント

C. Azure Monitor エージェント

D. Azure Pipelines エージェント

正解: **(**正解を表示します**)**

When a server is hosted outside of Azure (for example, in AWS , GCP , or on-premises), it must first be connected to Azure via Azure Arc before Microsoft Defender for Cloud can onboard it for protection and monitoring.
The Azure Arc agent (also known as the Connected Machine agent) establishes that connection between the non-Azure resource and Azure. Once connected, Defender for Cloud can then deploy the necessary security extensions and agents (such as the Defender for Endpoint sensor or vulnerability scanner) automatically.
Why not the other options:
* Microsoft Monitoring Agent (MMA): Legacy; replaced by the Azure Monitor Agent (AMA) and no longer required for new Defender deployments.
* Azure Monitor Agent (AMA): Used after Arc onboarding for data collection but cannot onboard non- Azure servers by itself.
* Azure Pipelines Agent: Used for Azure DevOps CI/CD, not for Defender for Cloud.
# Correct Answer: B. the Azure Arc agent

質問**: 77**
お客様は、Microsoft Defender for Endpoint Plan Zを使用するMicrosoft 365サブスクリプションをご利用で、1,000台のWindowsデバイスが含まれています。
デジタル署名された Script Vps1」という名前のPowerShellスクリプトがあります。
いずれかのデバイス上で、ライブレスポンスセッション中にScript1.pslを実行できることを確認する必要があります。
ライブレスポンスセッションで最初にすべきことは何ですか？
A. ライブラリコマンドを実行します。
B. putfileコマンドを実行します
C. デバイスの PowerShell 実行ポリシーを変更します。
D. Script1.ps 1 をライブラリにアップロードします。
正解**: (**正解を表示します**)**
In Microsoft Defender for Endpoint (MDE) live response sessions, to execute a PowerShell or other script on a remote device, the file must first be uploaded to the device from your local session. Microsoft documentation specifies that the putfile command is used to transfer a file (such as a script, tool, or executable) from the analyst's workstation to the target device's temporary working directory for execution.
Even though Script1.ps1 is digitally signed, Defender for Endpoint live response does not automatically access files from local storage or network paths. The analyst must explicitly upload the script using putfile , after which it can be executed within the live response shell.
The library and upload to library commands are used for storing reusable scripts centrally in the Microsoft Defender portal, but that's not required for a single manual session. Modifying the PowerShell execution policy is unnecessary because MDE live response sessions already allow executing approved scripts.
Hence, to minimize administrative effort and successfully run Script1.ps1 in the live session, the correct first action is:
B). Run the putfile command.

質問**: 78**
Azure Sentinel の要件を満たすテスト ルールを作成する必要があります。ルールを作成する際に、どのような手順を踏むべきですか？
A. セットルールロジックから、抑制をオフにします。
B. 分析ルールの詳細から、戦術を設定します。
C. セットルールロジックからエンティティをマッピングします。

D. アナリティクスルールの詳細から、重要度を設定します。

正解: **(**正解を表示します**)**

The test analytics rule must generate alerts for inbound Office 365 access by several test users and group those alerts into separate incidents-one per user . In Azure Sentinel, incident grouping by entity depends on the rule's Entity mapping . When you create a scheduled analytics rule, under Set rule logic you map columns from your query to entities like Account , IP , or Host . Once mapped, you can configure Event grouping so alerts with the same entity value (e.g., the same Account) are automatically grouped into a single incident.

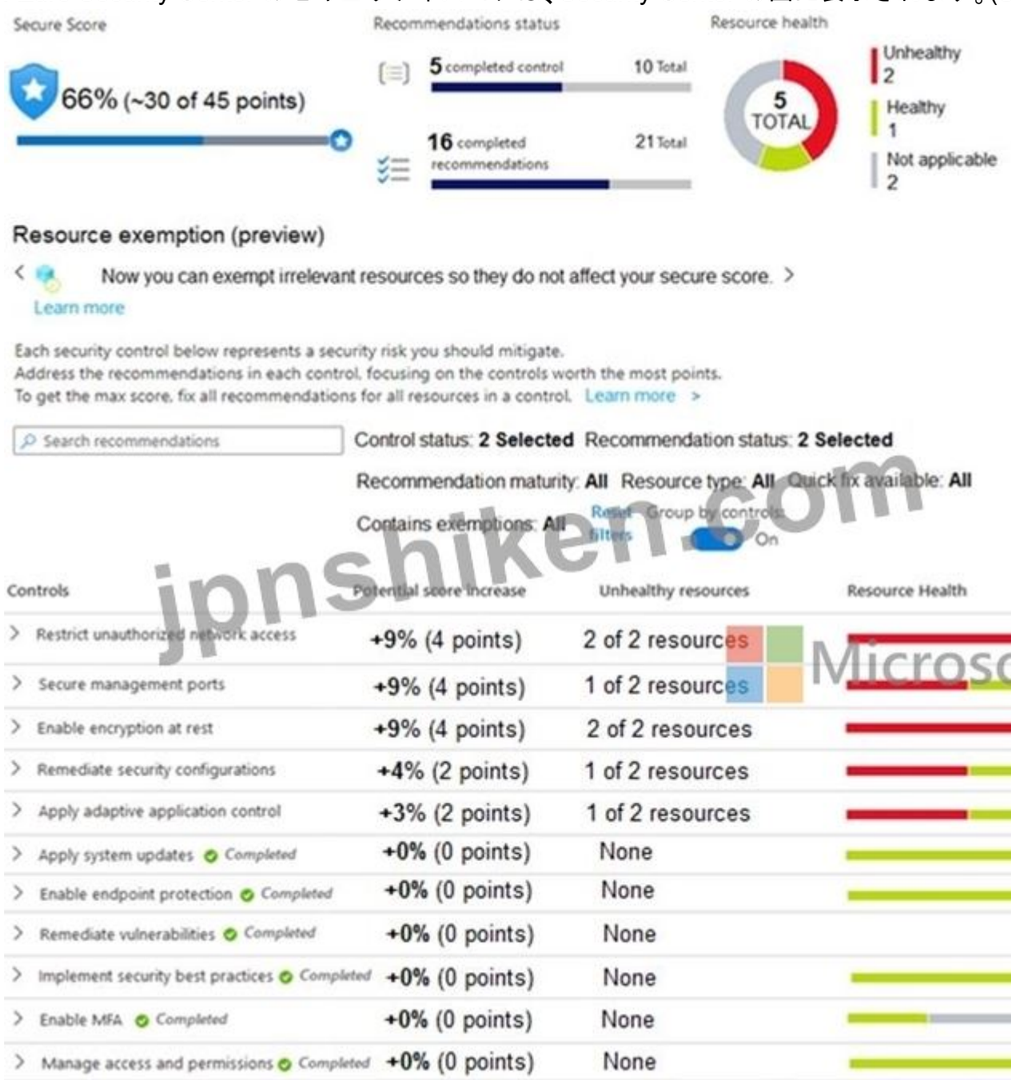
Turning suppression on/off or changing severity/tactics doesn't influence entity-based incident grouping.

Therefore, to ensure "one incident per test user account," you must map the Account entity (and any other relevant entities) in Set rule logic , then enable grouping by that entity-fulfilling the Sentinel requirement.

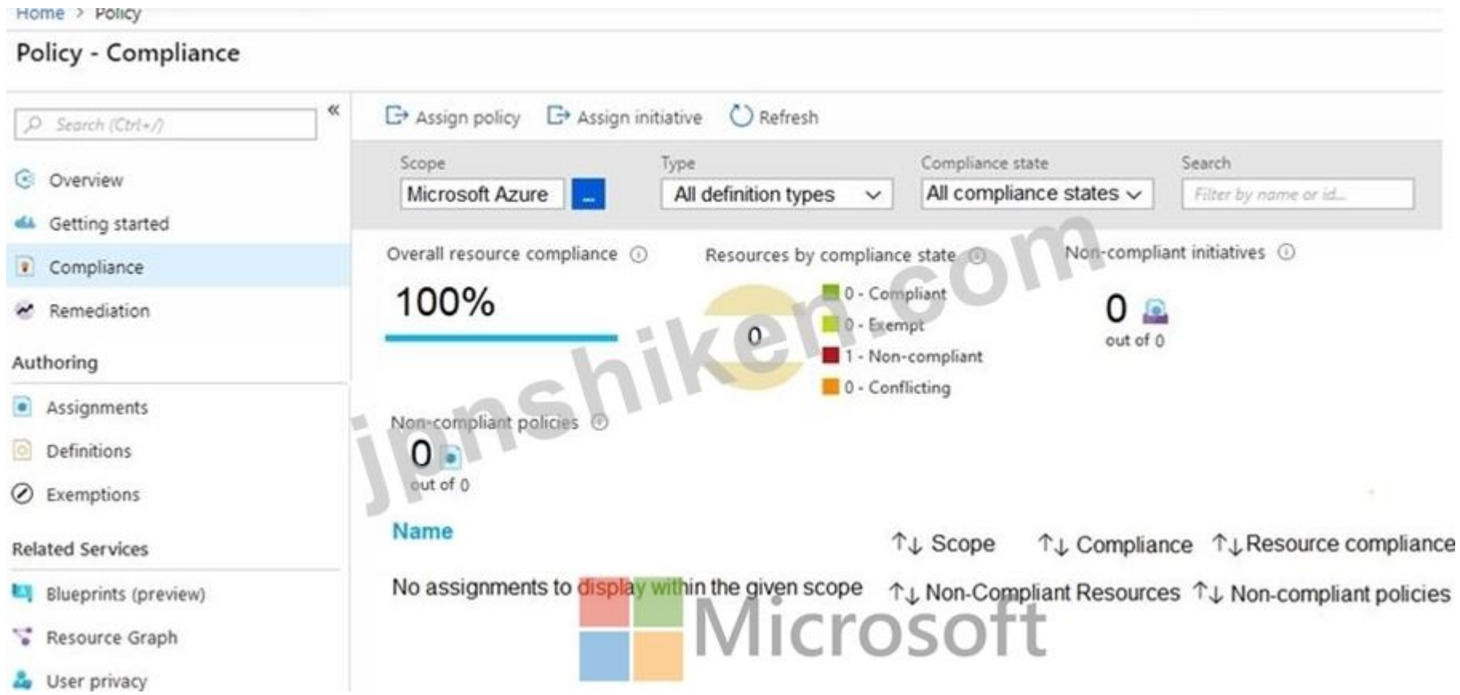
質問: **79**

あなたは、vm1とvm2という名前の2つの仮想マシンを含むAzureサブスクリプションのセキュリティ体制を管理します。

Azure Security Center のセキュリティスコアは、Security Center の図に表示されます。(Security Center タブをクリックしてください。)



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



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

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

正解:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Explanation:
Statements
Answer
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.
Yes
Both virtual machines have management ports exposed directly to the internet.
Yes
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four points.
Yes
In the Microsoft Defender for Cloud (Azure Security Center) screenshot, the Secure Score report shows several active security recommendations, including:
* " Restrict unauthorized network access " with a potential score increase of +9% (4 points) for 2 of 2 resources .
* " Secure management ports " with a potential score increase of +9% (4 points) for 1 of 2 resources .
These cont rols correspond to Defender for Cloud recommendations related to network security and exposure of management ports (RDP/SSH) . The fact that both controls show "2 of 2 resources" or "1 of 2 resources" as unhealthy means both virtual machines currently have NSG or firewall rules that allow inbound access from "Any" or "Internet ranges," indicating open ports and insecure configurations.
According to Microsoft documentation ("Improve your Secure Score in Microsoft Defender for Cloud"), enabling Just-In-Time (J IT) VM access mitigates these findings by restricting inbound RDP/SSH access to approved users for limited time windows, thereby increasing the Secure Score. Each remediated recommendation increases the Secure Score by the number of points shown in the "Po tential score increase" column (4 points in this case).
Because Azure Policy shows no assigned or conflicting policies , compliance enforcement is not yet active, confirming that the current exposure is due to lack of configuration rather than policy overri de.
Therefore:
* The two VMs have inbound Internet-accessible rules # Yes .
* They have management ports exposed # Yes .
* Enabling JIT network access would fix both recommendations, improving the Secure Score by 4 points
# Yes .

質問**: 80**
Microsoft Exchange Online と Microsoft Defender for Office 365 を使用する Microsoft 365 テナントがあります。
ゼロ時間自動パージ (ZAP) によってユーザーのメールボックスから電子メール メッセージが移動されたかどうかを識別するには、何を使用する必要がありますか?
A. Microsoft Defender for Office 365 の脅威保護ステータス レポート

B. Exchange のメールボックス監査ログ
C. Microsoft Defender for Office 365 の安全な添付ファイルのファイルの種類のレポート
D. Exchange のメール フロー レポート
正解: **(**正解を表示します**)**
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?
view=o365-worldwide

質問: **81**
Azure DevOps 組織があり、その中に Repo1 という名前の Azure Repos リポジトリがあり、Microsoft Defender for DevOps にオンボーディングされています。
インフラストラクチャ ・アズ ・コード(IaC)ファイルを作成し、Repo1に保存します。IaCファイルは、BicepファイルとHelmチャートの形式でフォーマットされます。
IaCファイル内の設定ミスを特定するには、Defender for DevOpsを設定する必要があります。
ファイルの種類ごとに、どのスキャンツールを使用すべきでしょうか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

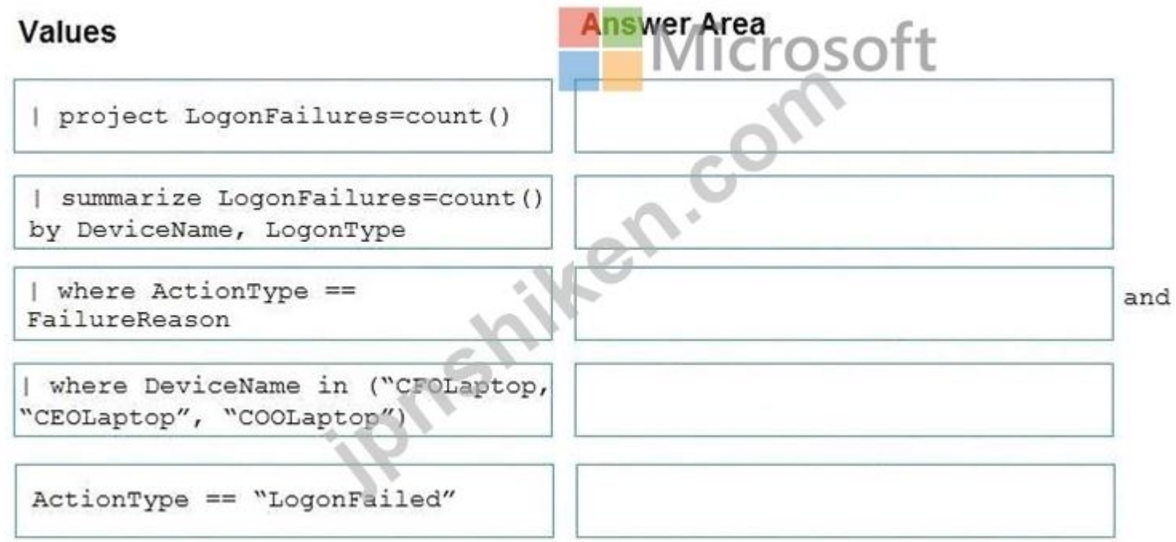
正解:

Explanation:

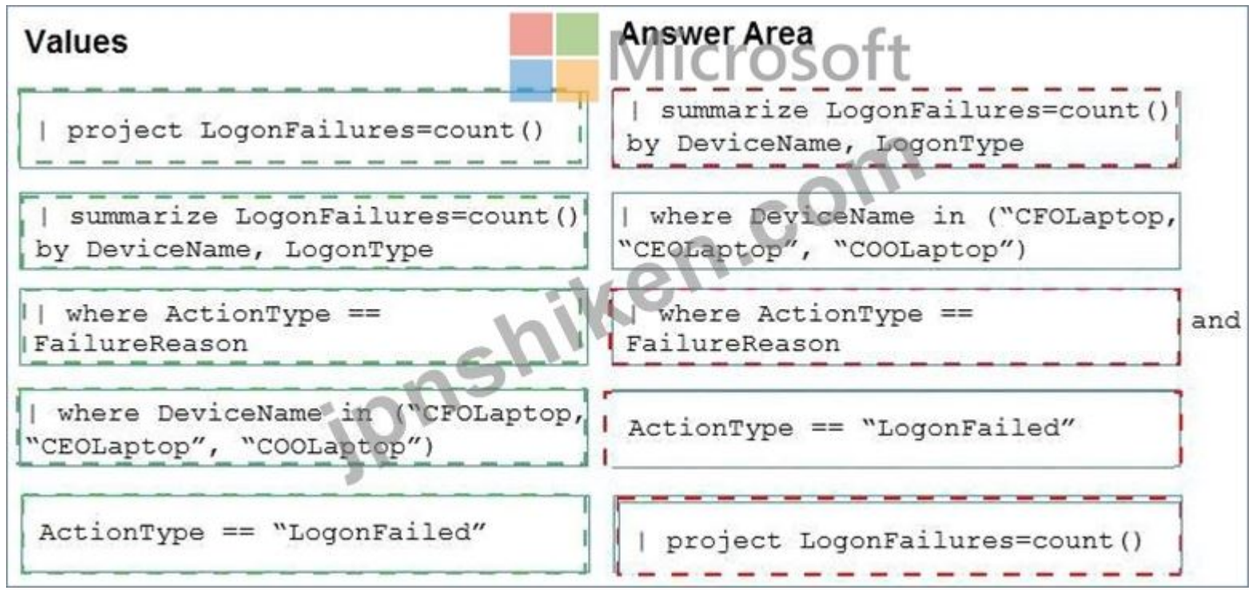
In Microsoft Defender for DevOps, IaC misconfiguration scanning uses purp ose-built analyzers per template type. For Azure Resource Manager (ARM) and Bicep templates, Defender leverages Template Analyzer , which evaluates security best practices and policy compliance specific to Azure resource definitions.

Template Analyzer parse s Bicep (and ARM JSON) and flags insecure defaults such as overly permissive network rules, missing encryption settings, insecure identity assignments, and more-making it the correct choice for Bicep files .
For container and Kubernetes ecosystem artifacts, including Helm charts , Defender integrates Terrascan , an open-source static analysis tool that scans Helm/Kubernetes manifests (and Terraform) against hundreds of policies. Terrascan inspects rendered Helm templates to detect issues like privileged contai ners, hostPath mounts, missing resource limits, and insecure service exposures.
By contrast, CredScan (Credential Scanner) is aimed at finding embedded secrets (keys/passwords) in code and isn't the primary IaC misconfiguration engine for either Bicep or H elm in Defender for DevOps.
Therefore, to detect IaC misconfigurations: use Template Analyzer for Bicep and Terrascan for Helm charts .

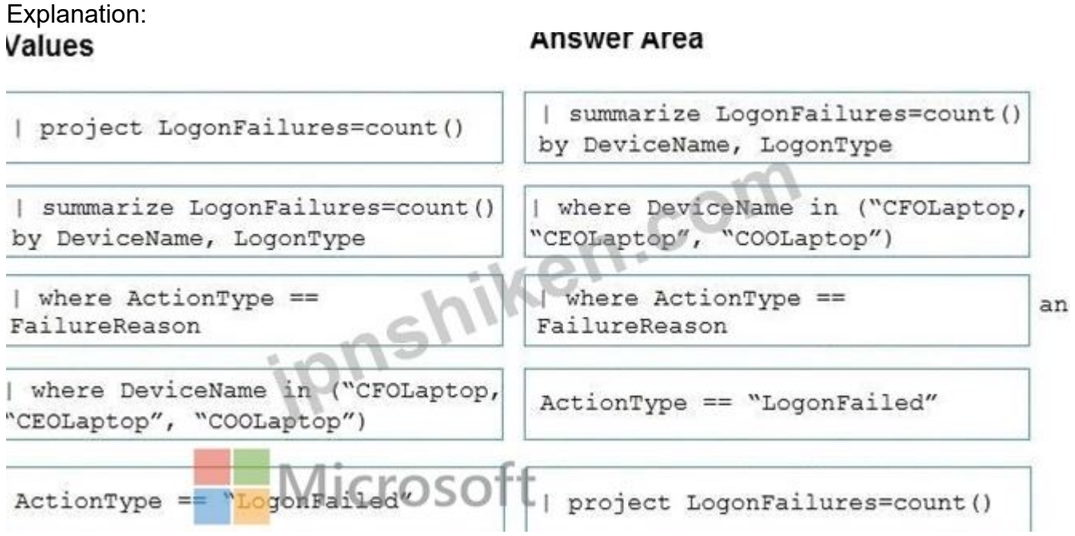
質問: **82**
あなたはMicrosoft 365 Defenderを使用してインシデントを調査しています。
CFOLaptop、CEOLaptop、COOLaptopという名前の3つのデバイスで、サインイン認証の失敗を検出するために、高度なハンティングクエリを作成する必要があります。
クエリをどのように完了すればよいですか? 回答するには、回答の適切なオプションを選択してください。a.
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



In Microsoft 365 Defender's Advanced Hunting (Kusto Query Language - KQL) , investigators use the DeviceLogonEvents table to search for authentication attempts and filter failed logons. To detect failed sign- ins from specific devices, you begin by applying a where clause that filters only the relevant logon failures and the specific device names you want to investigate.

The correct syntax and logical order-based on Microsoft Security Operations (SecOps) and Microsoft 365 Defender hunting guide -is to first filter (where) the Ac tionType to "LogonFailed," then narrow down the dataset to the target devices (DeviceName in (" CFOLaptop " , " CEOLaptop " , " COOLaptop ")). This ensures that only failed authentication attempts from those three machines are included.

After filtering, the summarize operator is used to group the data by DeviceName and LogonType , counting how many failures occurred per device and logon type. This aggregation step follows Microsoft's recommended practice for incident hunting, allowing analysts to quickly assess which devices are generating unusual authentication failure volumes.

Finally, the project statement selects only the LogonFailures output, simplifying the results for reporting or alerting purposes.

This query structure aligns exactly with Microsoft 365 Defender Advanced Hunting documentation for detecting failed logins on specific endpoints while maintaining query efficiency and clarity, minimizing administrative overhead during investigations

質問: **83**

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上で悪意のある活動を検知しました。
デバイス1でライブレスポンスセッションを開始します。
以下の操作を実行する必要があります。
* ライブレスポンスライブラリからファイルをダウンロードします。
* Device1で実行中のプロセスを停止します。
各アクションに対して、どのライブレスポンスコマンドを実行すべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

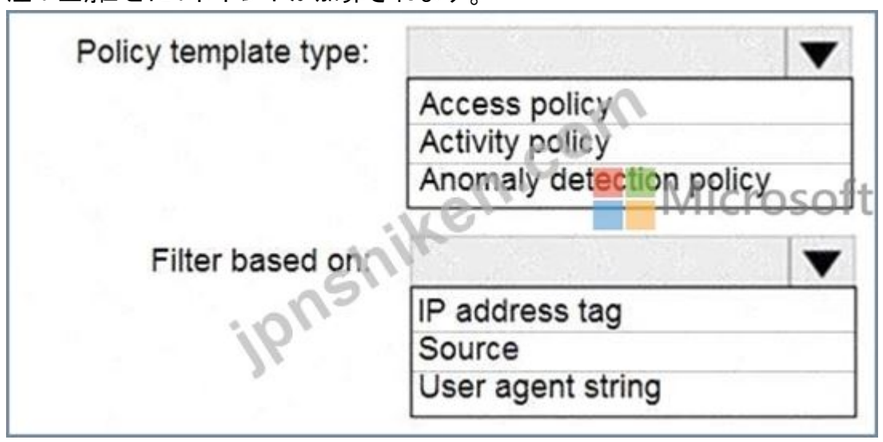
Answer Area

Explanation:

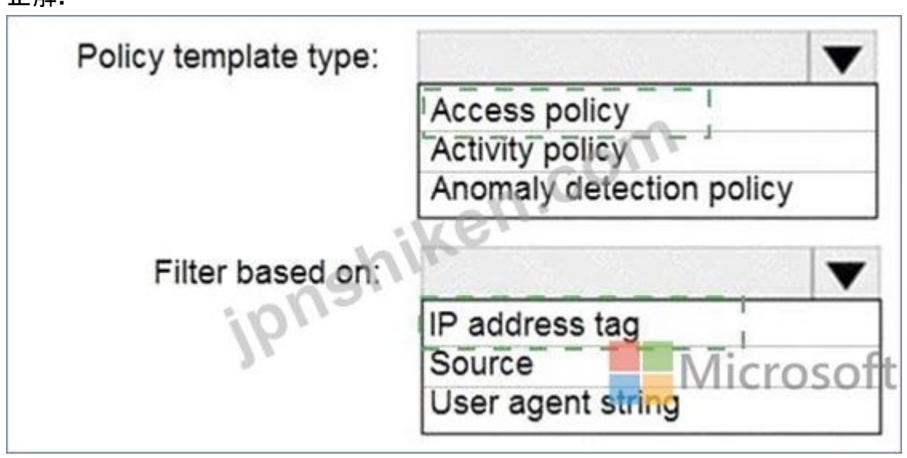
In Microsoft Defender for Endpoint live response sessions, specific commands are provided to perform investigation and remediation tasks directly on a device. According to the official Defender for Endpoint documentation:
* The getfile command is used to download a file from the live response library to the local analyst's session. This command enables investigators to retrieve files that are stored in the Defender live response library for examination or comparison. The command is explicitly documented as "Retrieves a file from the library or from the device."

* The remediate command is used to take action against threats detected on the endpoint, such as stopping processes, deleting files, or quarantining malware. The remediation commands are part of the live response toolkit and provide direct control over running processes or malicious files during an active incident response session.
Other commands serve different purposes:
* library lists th e available files in the live response library.
* putfile uploads files to the library.
* analyze runs advanced analysis tasks.
* services lists or manages Windows services but is not used to stop arbitrary processes.
Therefore, for this scenario, the correct li ve response commands are:
* Download a file from the live response library: getfile
* Stop a process that is running on Device1: remediate

質問**: 84**
Microsoft 365のサブスクリプションを購入します。
Microsoft Cloud App Security を構成する予定です。
ボットネットネットワークから発信されたMicrosoft 365アプリへの接続を検出する、カスタムテンプレートベースのポリシーを作成する必要があります。
何を使用すべきですか？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:

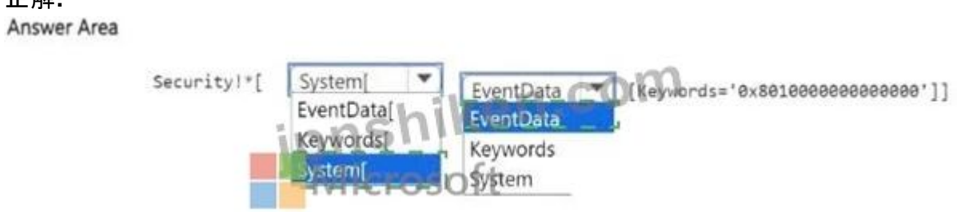


Explanation:
Policy template type: Access policy
Filter based on: IP address tag
In Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security), policies are used to detect, alert, and control access or activity patterns across cloud applications.
To detect connections originating from a botnet network , you need a policy that evaluates real-time access conditions such as the user's IP address, device, or location at the time of the connection attempt.
This is achieved thr ough an Access policy , which controls and monitors session access to cloud apps using Conditional Access App Control.
Microsoft documentation specifies that Access policies can filter based on IP address ranges, tags, or risk levels. The "IP address tag" i s particularly used to classify addresses into categories like "Risky," "Anonymous proxy," "Botnet," etc. Microsoft's built-in IP address tagging capability recognizes malicious or suspicious sources, including known botnet IPs.
* Activity policies monitor i n-app user actions such as file downloads, sharing, or admin operations- not the connection origin.
* Anomaly detection policies rely on behavioral analytics and machine learning, not static IP classifications, and cannot explicitly target botnet IPs.
Therefo re, to meet the requirement of detecting connections to Microsoft 365 apps from botnet networks , you must configure an Access policy that filters based on the IP address tag set to "Botnet."

質問**: 85**
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**)**
In Microsoft Sentinel, a custom analytics (scheduled) rule can fail intermittently for transient reasons.
According to Microsoft's guidance on troubleshooting analytics rules:
* A transient failure is one that occurs due to a temporary condition and does not require human intervention to resolve. Examples include: * The rule query takes too long to run and times out. * Connectivity issues between the data sources and Log Analytics, or between Log Analytics and Microsoft Sentinel.Microsoft Sentinel will attempt to run the rule again after a delay, up to predetermined retries.
Therefore, option A (rule query taking too long) and option D (connectivity issues) are correct causes of intermittent failures.
On the other hand, permanent failures or configuration-level issues can lead to rules being "auto-disabled," but those are not intermittent failures. The documentation lists permanent failure causes like the target workspace being deleted or permissions to data sources being changed. Microsoft Learn For example:
* Option B (the target workspace was deleted) is a permanent cause, not an intermittent one. Once the workspace is gone, the rule can never run.
* Option C (permissions to the data sources of the rule query were modified) is also a permanent failure scenario, because once permissions change, the rule loses access until corrected, which is not something that happens intermittently unless someone is repeatedly toggling permissions.

質問**: 86**
Sub1 という名前の Azure サブスクリプションがあります。Sub1 には、SW1 という名前の Microsoft Sentinel ワークスペースと、Windows Server を実行する VM1 という名前の仮想マシンが含まれています。SW1 は、AMA コネクタを介して Windows セキュリティ イベントを使用して、VM1 からセキュリティ ログを収集します。
VM1から収集するイベントの範囲を制限する必要があります。ソリューションは、監査失敗イベントのみが収集されるようにする必要があります。
コネクタのフィルタ式はどのように完成させるべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:



Explanation:

In Microsoft Sentinel, when using the Windows Security Events via AMA (Azure Monit or Agent) connector, you can configure an XPath filter expression to control which Windows security events are collected from a connected virtual machine.

Microsoft's documentation specifies that event filtering is based on the EventLog XML schema , and filtering by Keywords allows you to target specific audit categories. In Windows Security logs, events are categorized as follows by their Keywords bitmask :

* 0x8020000000000000 # Audit Success events
* 0x8010000000000000 # Audit Failure events

Since the requirement is to collect only audit failure events , the XPath filter must include only the System node (which contains the event header metadata) and filter by the Keywords attribute equal to 0x8010000000000000 .

The correct XPath syntax for the filter in this case is:

Security!*[System[Keywords= ' 0x8010000000000000 ']]

Explanation of components:

* Security! * - Targets the Windows Security event log.
* System[...] - Refers to the event's header metadata section (where Keywords, EventID, and Level are stored).
* Key words= ' 0x8010000000000000 ' - Matches only events that have the Audit Failure bit set.

Therefore, only events with Audit Failure outcomes will be collected from VM1, satisfying the requirement to minimize event ingestion and reduce unnecessary log noise.

Final Answer: Security!*[System[Keywords= ' 0x8010000000000000 ']]

質問**: 87**

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 Filel という名前のファイルとしてエクスポートします。

10,000行を含むCSVファイル。

Microsoft Excelを使用して、Filel.csvファイルから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。

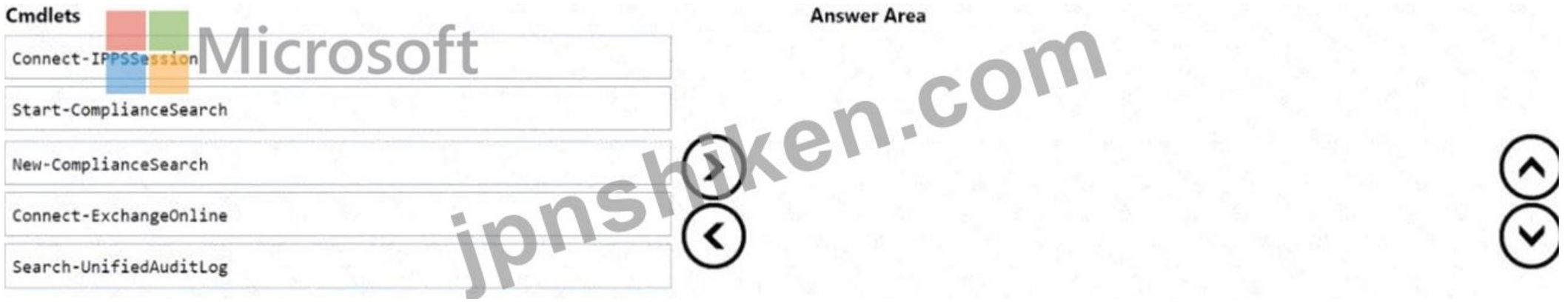
監査検索結果において、Excelが特定のJSONプロパティに対応する列を生成するようにする必要があります。

解決策 :ExcelからFilel.csvの既存の列にフィルターを適用して行数を減らし、次に データの取得と変換」操作を実行してAuditData列を解析します。

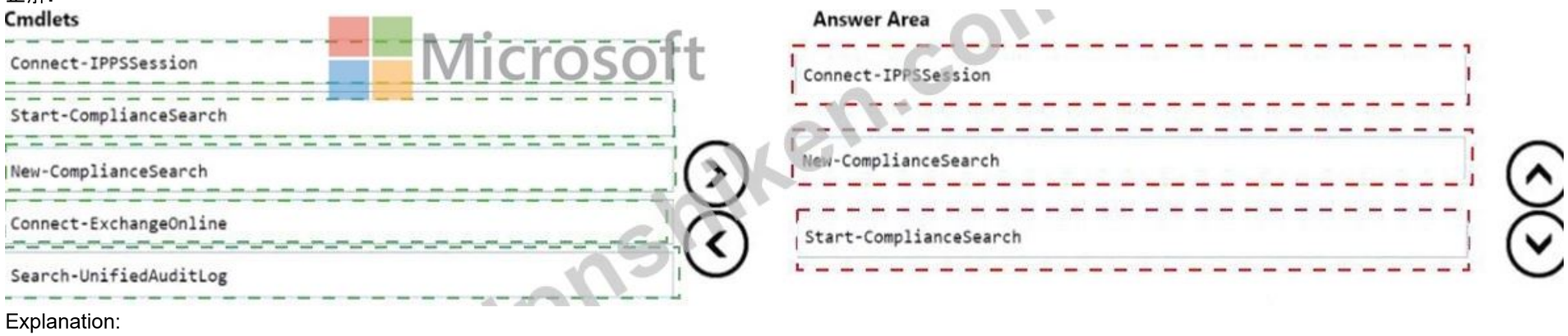
これは要件を満たしていますか？
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
This solution also does not meet the requirement. Applying filters to the already-imported worksheet rows in Excel (or attempting to reduce rows in the workbook UI) does not change how Power Query initially samples and infers the JSON schema during the Get & Transform steps. Power Query's schema detection typically happens on a preview/sample of the source data when the query is first evaluated. If the JSON property you need does not appear in that sampled subset, P ower Query will not create a column for it even if you later filter the data to include rows that do contain that property. In short, post-export filtering in Excel is not a reliable way to force Power Query to detect and expand missing JSON properties.
Th e reliable approaches are to increase the number of rows Power Query uses for schema detection (Query Options / Data Load / preview/sample settings) or to explicitly parse each AuditData cell with JSON.
Document (or equivalent M functions) and then expand t he record fields-these approaches ensure the specific JSON properties are surfaced as columns. Reducing rows via Excel filters does not address the sampling/schema-detection behavior and therefore fails to satisfy the requirement.

質問: **88**
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: **(**正解を表示します**)**
In Microsoft Sentinel, playbooks are Azure Logic Apps that automate responses to alerts or incidents. To use an existing Logic App as a playbook in Sentinel, it must start with the "Microsoft Sentinel alert" trigger.
This trigger allows Sentinel to call and pass alert details to the Logic App automatically.
When an existing Logic App has a manual trigger, it cannot be invoked directly by Sentinel. Therefore, the first step is to modify the trigger to replace the manual trigger with the "When a response to an Azure Sentinel alert is triggered" trigger. After that, you can link it within Sentinel incidents or automation rules.
This process is detailed in Microsoft Defender XDR and Sentinel documentation under "Connect a Logic App to Sentinel as a playbook." Hence, the correct answer is D. Modify the trigger in the logic app.

質問: **89**
お客様は、Microsoft Exchange Onlineを使用するMicrosoft 365 E5サブスクリプションをお持ちです。
フィッシングメールを識別する必要があります。
どの 3 つのコマンドレットを順番に実行する必要がありますか？回答するには、コマンドレットの一覧から適切なコマンドレットを回答欄に移動し、正しい順序に並べ替えてください。



正解:



Explanation:

1# # Connect-IPPSSession

2# # New-ComplianceSearch

3# # Start-ComplianceSearch

In Microsoft 365 E5 (which includes Microsoft Purview and Exchange Online), to identify phishing email messages using PowerShell, administrators can perform a compliance content search . The process requires connecting to the Microsoft Purview (Security & Compliance Center) PowerShell and then creating and running a compliance search.

Here's the correct order and purpose of each cmdlet:

1# # Connect-IPPSSession

* This cmdlet establishes a remote PowerShell session to the Microsoft Purview Compliance Center (formerly Security & Compliance Center) .
* It's required before executing any compliance-related PowerShell commands such as creating or starting a search.
* Example:
* Connect-IPPSSession

2# # New-ComplianceSearch

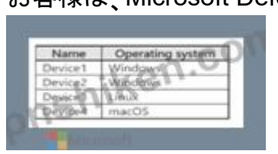
* After connecting, use this cmdlet to create a new compliance content search .
* You can define parameters such as the search name, target locations (e.g., all mailboxes or specific users), and search query (for example, filtering by suspected phishing keywords or sender domains).
* Example:
* New-ComplianceSearch -Name " PhishingSearch " -ExchangeLocation All -ContentMatchQuery ' Subject: " phish " OR Subject: " urgent action required " '

3# # Start-ComplianceSearch

* Once the search is defined, this cmdlet initiates the compliance search to scan the selected mailboxes for phishing-related messages.
* Example:

* Start-ComplianceSearch -Identity " PhishingSearch "
Other cmdlets explained:
* Connect-ExchangeOnline is used for managing Exchange Online configuration, not compliance or content searches.
* Search-UnifiedAuditLog searches the unified audit log , which is used for activity auditing, not email content searches.
# Final Correct Sequence:
* Connect-IPPSSession
* New-ComplianceSearch
* Start-ComplianceSearch

質問: **90**
App1 の Microsoft Sentinel 要件を満たす必要があります。App1 では何を構成すればよいですか？
A. API接続
B. トリガー
C. コネクタ
D. 認証
正解: **(正解を表示します)**
In Microsoft Sentinel, data from applications, security solutions, and services is ingested through data connectors . To integrate App1 with Sentinel and meet its monitoring or data ingestion requirements, you must configure a connector .
Microsoft Sentinel documentation specifies:
"Data connectors provide the integration point between Microsoft Sentinel and other data sources, including Microsoft services, third-party solutions, and custom applications." Connectors manage authentication, data formats, and continuous ingestion of logs or alerts into Sentinel's Log Analytics workspace.
Other options:
* API connection - supports Logic Apps but not direct Sentinel ingestion.
* Trigger - used for playbooks or automation, not data ingestion.
* Authorization - a setting used within connectors or playbooks, not configured separately.
# Correct configuration for App1: a connector

質問: **91**
お客様は、Microsoft Defender for Endpointを使用するMicrosoft 365サブスクリプションをご利用で、以下の表に示すデバイスが含まれています。


各デバイス上でライブレスポンスセッションを開始します。
各デバイスからDefender for Endpointの調査パッケージを収集する必要があります。
コマンドラインインターフェース(CLI)から高度なライブレスポンスコマンドを実行することで、どのデバイスでパッケージを収集できますか？
A. デバイス1とデバイス2のみ
B. デバイス1、デバイス2、およびデバイス3のみ
C. デバイス3とデバイス4のみ
D. デバイス1、デバイス2、デバイス3、およびデバイス4
正解: **(正解を表示します)**

In Microsoft Defender for Endpoint (MDE) , a live response session allows security analysts to remotely connect to onboarded devices and run investigation commands. One of the key commands available is the ability to collect an investigation package , which includes forensic artifacts such as event logs, registry hives, running processes, network connections, and more.
According to Microsoft's official Defender for Endpoint documentation:
"Advanced live response capabilities, including running scripts and collecting investigation packages, are supported on Windows and Linux devices. macOS devices support basic live response commands only." This means that while Windows (Device1 and Device2) and Linux (Device3) devices fully support advanced live response capabilities (including collect investigation_package), macOS (Device4) devices currently support only a limited subset of commands-basic file and directory operations, without the ability to collect investigation packages.
Therefore:
* Device1 (Windows) # Supported
* Device2 (Windows) # Supported
* Device3 (Linux) # Supported
* Device4 (macOS) # Not supported
# Final answer: B. Device1, Device2, and Device3 only

質問: **92**
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。

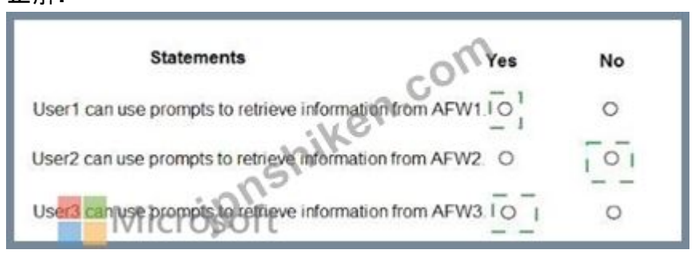
Name	Log configuration	Destination
AFW1	Unstructured logs	Log Analytics
AFW2	Structured intrusion detection and prevention system (IDPS) logs	Azure Event Hubs
AFW3	Structured intrusion detection and prevention system (IDPS) logs	Log Analytics

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。

正解:



Explanation:

Yes No Yes

According to Microsoft Copilot for Security and Defender for Cloud (Azure Firewall) integration guidance, Copilot can retrieve information from connected security data sources such as Log Analytics, Microsoft Sentinel, and Defender XDR. To access data via Copilot prompts, two conditions must be satisfied:

* The user must have the appropriate Copilot role (Owner or Contributor).
* The user must have the necessary Azure permissions (RBAC) to access the underlying data source or workspace (e.g., Log Analytics, Sentinel, or Azure Firewall logs).

User1 - Has the Contributor role at the subscription level , meaning full access to all resource groups and Log Analytics workspaces. As a Copilot Owner , User1 can query Copilot and retrieve data from AFW1 logs (which are in Log Analytics). Hence, Yes .

User2 - Also has Contributor rights at the subscription level but is only a Copilot Contributor . A Copilot Contributor can collaborate in sessions but cannot initiate or run data retrieval prompts independently. Therefore, No for AFW2.

User3 - Has the Security Reader role at the resource group level, providing read access to security data for that group, and is a Copilot Owner , enabling prompt access to connected security sources. Since AFW3 logs are in Log Analytics within the same resource group, User3 can retrieve data using Copilot. Thus, Yes .

Therefore, the correct answers are:

* User1 # Yes
* User2 # No
* User3 # Yes

質問: **93**

Microsoft Sentinelを使用します。

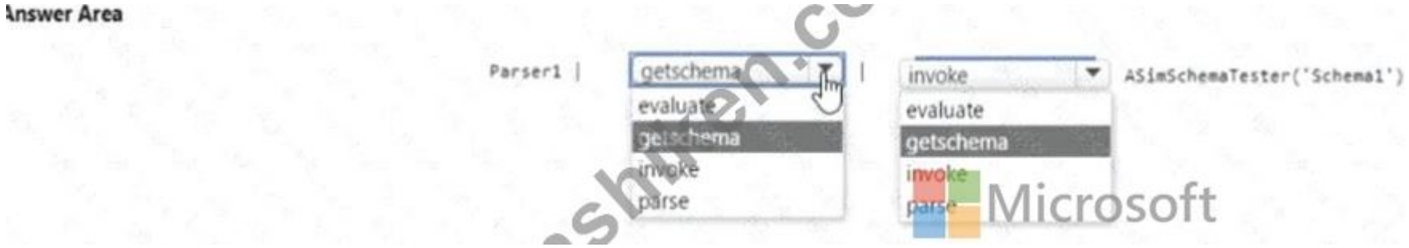
Azure Storage アカウント キーが列挙されるたびに、ほぼリアルタイムでアラートを受け取る必要があります。実行すべき 2 つのアクションはどれですか? 正解はそれぞれソリューションの一部を示しています。注: 正解ごとに 1 ポイントが加算されます。

A. ブックマークを作成します。
B. 分析ルールを作成します。
C. ライブストリームを作成します。
D. ハンティングクエリを作成します。
E. データコネクタを追加します。

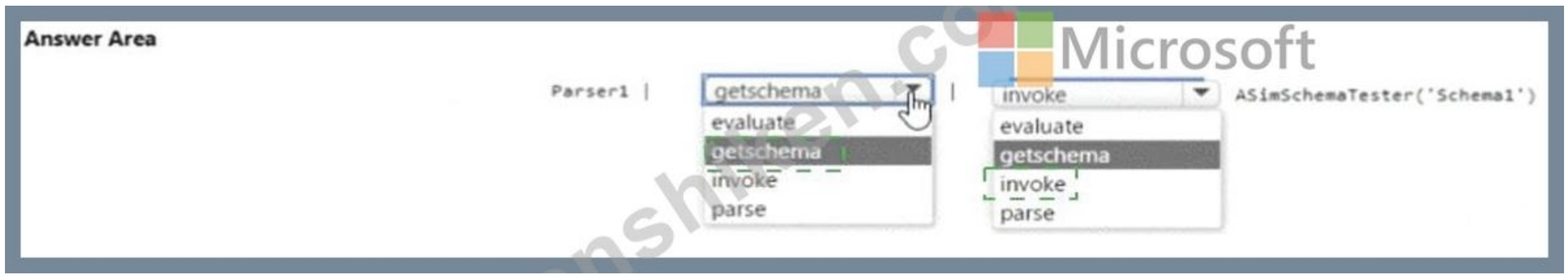
正解: **(**正解を表示します**)**

In Microsoft Sentinel, to receive near real-time alerts when specific activities occur-such as Azure Storage account key enumeration -you combine two Sentinel capabilities: Livestream and Analytics rules .
* Livestream provides real-time monitoring of events based on KQL q ueries. According to Microsoft Sentinel documentation, Livestream "lets you run queries continuously and get notified immediately when results match specific conditions." This allows SOC analysts to detect ongoing attacks (such as credential enumeration) a s they happen.
* Analytics rules provide ongoing automated monitoring and alerting. A scheduled analytics rule runs periodically (for example, every 5 minutes) and gen erates an alert when a defined condition is met.
The "Storage account keys enumerated" even t comes from Microsoft Defender for Cloud (or Azure Activity) logs, so you can define a KQL-based rule to detect these activities.
Therefore:
* B (Analytics rule): to automatically generate alerts when the condition is met.
* C (Livestream): to receive those a lerts or detections in near real-time as they occur.
Together, these meet the requirement for near real-time detection and alerting with minimal manual monitoring.

質問**: 94**
Microsoft Sentinelワークスペースをお持ちです
Parser1という名前のカスタムAdvanced Security Information Model(ASIM)パーサーを開発し、Schema1という名前のスキーマを生成させます。
Schema1を検証する必要があります。
このコマンドをどのように完了すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。
Answer Area



正解:



Explanation:

To validate a custom ASIM parser output, you test that the parser's resulting table structure complies with the intended ASIM schema . In KQL, the getschema operator produces a tabular representation of the current pipeline's schema (column names, types, order). The invoke operator is then used to call a function on that tabular input. ASIM provides the helper function ASimSchemaTester() , which accepts the schema table and the target schema name and validates that the input conforms (columns exist, types match, required fields are present).

Therefore, the correct construction is to run the parser (here, Parser1), pipe its output to getsch ema to obtain the schema of the produced table, and then invoke ASimSchemaTester(' Schema1 ') to perform the validation. Other options are not appropriate: evaluate is for plugins; parse extracts fields from strings rather than validate schema; and calling the tester without getschema would not pass the required schema table.
Hence, the correct command is:
Parser1 | getschema | invoke ASimSchemaTester(' Schema1 ') .

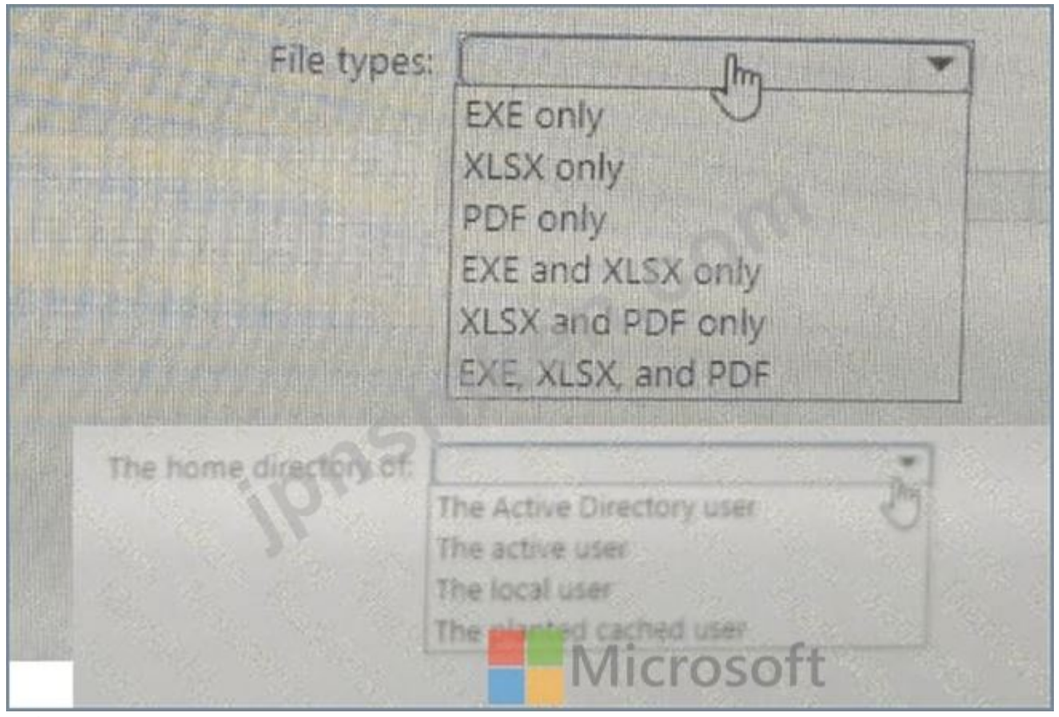
質問: **95**
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
以下の要件を満たすKQLのハンティングクエリを作成する必要があります。
* 過去 12 時間以内に File1.pdf という名前の添付ファイルを含むメールを受信し、その添付ファイルを開いたデバイスを特定します。
クエリの実行に必要なリソースを最小限に抑えます。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

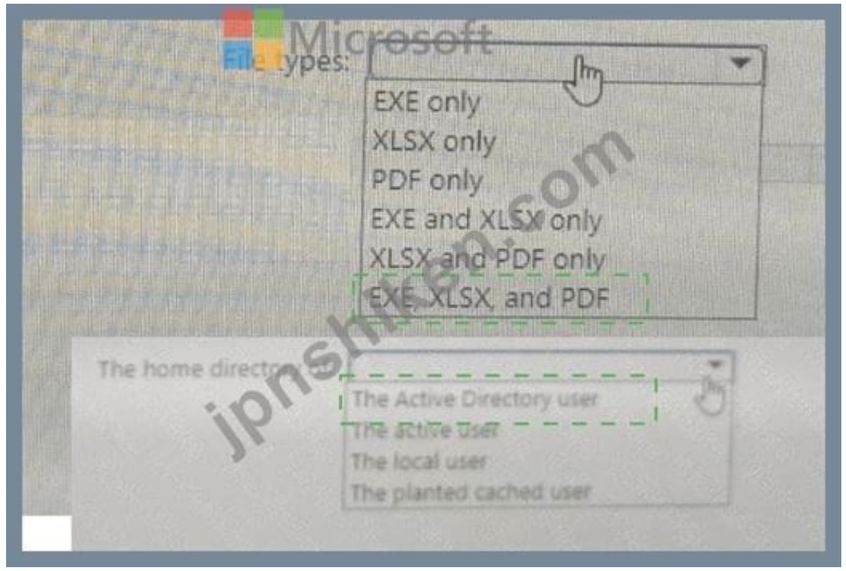
Explanation:

In Microsoft Defender XDR hunting, EmailAttachmentInfo includes metadata for received attachments (name, subject, and the file's SHA256), while DeviceFileEvents records file operations on endpoints (open
/read/execute) and also carries the SHA256 hash. Microsoft's guidance for efficient joins in KQL recommends correlating artifacts using stable, high-cardinality identifiers (hashes) rather than paths or URLs, becau se paths can change and URLs may not be preserved on disk; hashes uniquely identify the same file across mail and endpoint telemetry. To minimize query resources , Kusto's join kind=innerunique is preferred when the left side (EmailAttachmentInfo) is expect ed to have unique keys (one attachment hash per message instance) and you want at most one match per left record. It reduces shuffle/duplication compared to inner , improving performance while returning only devices that actually opened the same file (by ma tching SHA256) within the last 12 hours.
So the optimal query structure is:
EmailAttachmentInfo
| where Timestamp > ago(12h)
| where Subject == " Document Attachment " and FileName == " File1.pdf "
| join kind=innerunique
(DeviceFileEvents | where Timestamp > ago(12h))
on SHA256
This precisely identifies devices that received the email with File1.pdf and opened that same file, using the most efficient join strategy and a reliable correlation key.

質問: **96**
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:



Explanation:

You're configuring a Deception rule in Microsoft Defender XDR and need to provide a custom lure file .

* You set the Planting path to HOME , which means the file will be deployed into user home directories.

You must determine:

* Which file types are supported for custom lure files.
* Which home directory the file should reside in.

1. File types that can be used for a custom lure # Verified Answer = EXE, XLSX, and PDF As per Microsoft Defender for Endpoint Deception documentation:

"Custom lure files can be created using EXE, XLSX, or PDF file types. These file types are supported for deception scenarios and can trigger alerts when accessed or executed by an attacker." The platform uses these file types because they are commonly interacted with by adversaries during lateral movement or reconnaissance.
* EXE : Simulates executables that appear valuable or tempting.
* XLSX / PDF : Represent business-related or sensitive document lures.
Therefore, you can upload EXE, XLSX, and PDF lure files simultaneously or select one of them.
Correct selection: EXE, XLSX, and PDF
2. Home directory the file should be located in # Verified Answer = The active user When you set the Planting path = HOME , Defender plants the deception artifact (lure file) under the active user's home directory .
This ensures that the lure file is visible and accessible within the context of the currently logged-in user- precisely where attackers are most likely to browse or exfiltrate files.
According to Microsoft's deception feature reference:
"When the planting path is set to HOME, the deception files are placed in the home directory of the active user on the device. This ensures that the files are visible during an interactive session and accessible to adversaries using that account." Other options such as "Active Directory user," "Local user," or "Planted cached user" are not used for standard HOME planting. The deception system targets the context of the active session to maximize effectiveness and reduce false positives.
Correct selection: The active user
Final Verified Answers: Configuration Aspect
Correct Option
File types:
EXE, XLSX, and PDF
Home directory of:
The active user
Summary:
When creating a custom lure file in Microsoft Defender XDR Deception with the planting path set to HOME , you should:
* Use EXE, XLSX, and PDF file types.
* Place them in the active user's home directory on the target device.
These selections align with Microsoft Defender XDR Deception's official documentation and M365 E5 SecOps study material.
Question Part 1: Which types of files can you use for the custom lure?
The Answer:
EXE, XLSX, and PDF
According to your screenshot (File types drop-down), you can use the following file types for a custom lure in Microsoft Defender XDR deception rules:
* EXE
* XLSX
* PDF
You can select any combination of these, so EXE, XLSX, and PDF are all supported as custom lure file types.

質問**: 97**
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。
あなたはAzDO1という名前のAzure DevOps組織を持っています。
Sub!とAzDO1を統合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。
* Defender for Cloudを使用して、パイプライン内で公開されている機密情報を検出します。
管理業務の手間を最小限に抑える。

正解:

Explanation:

To integrate Microsoft Defender for Cloud with Azure DevOps (AzDO1) for detecting secrets exposed in pipelines , you must connect the two platforms using Microsoft's built-in integration flow that enables Defender for Cloud to scan repositories and pipelines for vulnerabilities and sensitive data exposure.

Here's the correct configuration process:

Step 1: In Defender for Cloud - Add an environment In the Defender for Cloud portal, you first need to add an environment that represents your Azure DevOps organization.

This step connects Defender for Cloud to the DevOps service, allowing it to monitor repositories, build pipelines, and artifacts.

* Navigate to Defender for Cloud # Environment settings # Add environment # Azure DevOps .
* You'll then authenticate your Azure DevOps organization (AzDO1) to allow Defender for Cloud to scan your pipelines.

This setup enables Defender for DevOps , a capability within Defender for Cloud, to detect exposed secrets, insecure dependencies, and misconfigurations directly from pipeline activities.

Step 2: In AzDO1 - Install an extension Next, within Azure DevOps (AzDO1) , install the Microsoft Defender for DevOps Security Scanner extension from the Azure DevOps Marketplace .

This extension integrates the Defender for Cloud scanning engine into the Azure DevOps pipeline process and enables automatic scanning for:

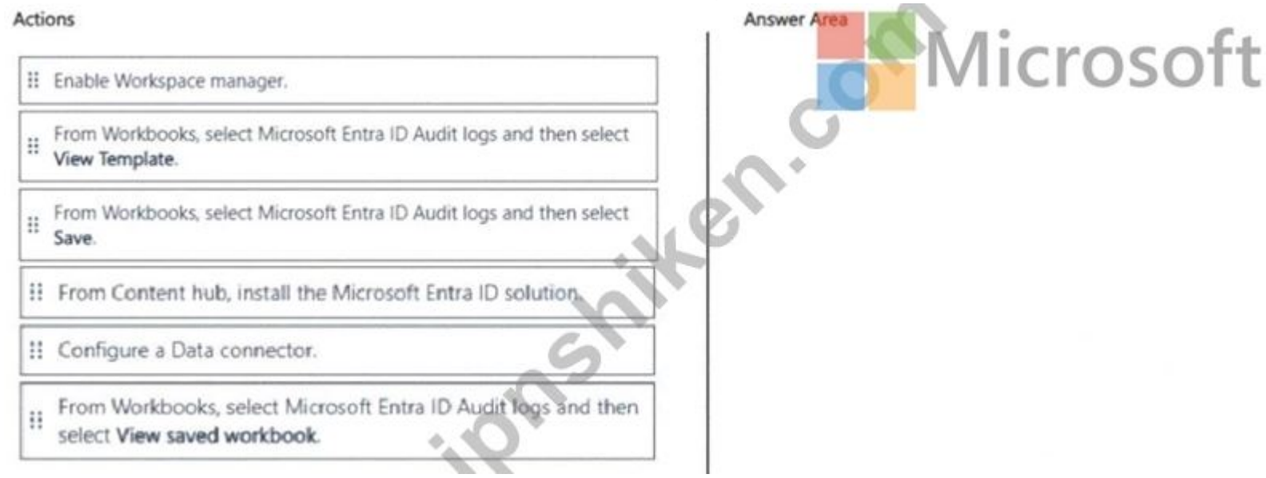
* Hardcoded secrets in YAML pipelines,
* Vulnerability findings in open-source dependencies, and
* Infrastructure-as-code misconfigurations (for example, ARM, Terraform).

Once installed, the extension automatically works with Defender for Cloud, and any detected secret exposure or security issue is surfaced in Defender for Cloud's "DevOps Security" dashboard.

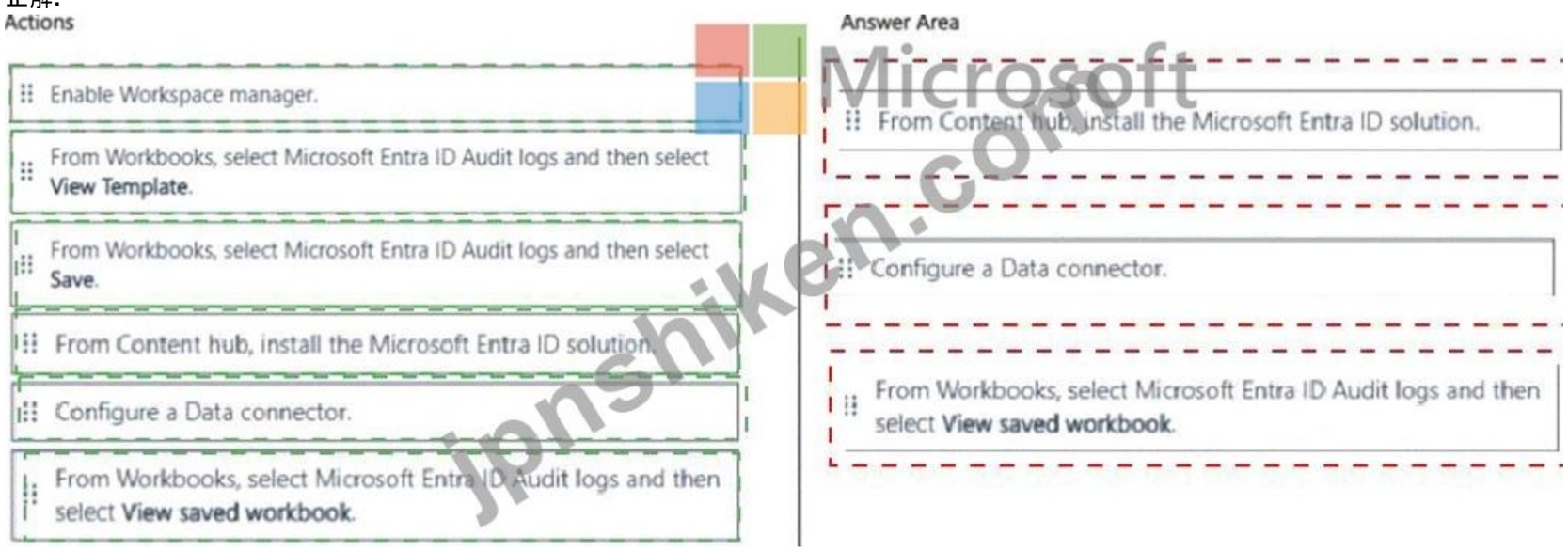
* Configure workflow automation: Applies to automated incident responses, not DevOps integration.
* Enable a plan: Refers to enabling Defender plans for specific Azure resource types, not connecting DevOps.

* Configure OAuth / Configure security policies: Required for custom integration scenarios, but not for standard Defender-DevOps onboarding.
Why Other Options Are Incorrect:
Final Correct Answer:
* In Defender for Cloud: Add an environment
* In AzDO1: Install an extension

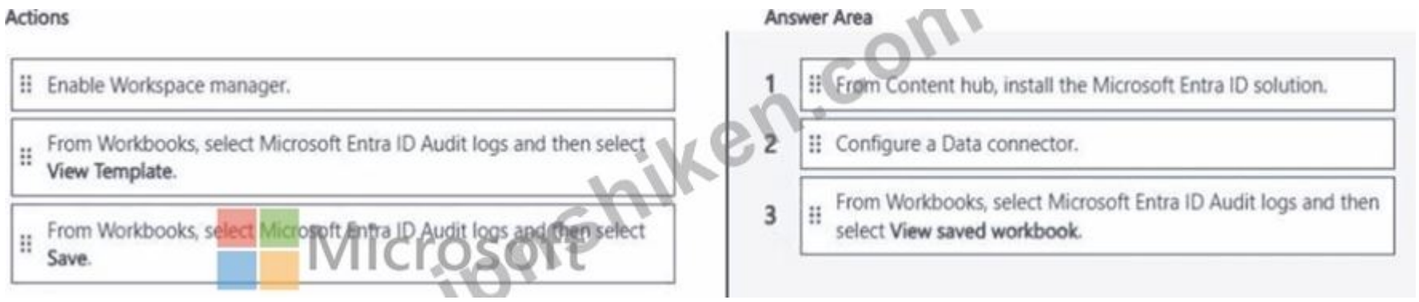
質問: **98**
Microsoft Sentinelワークスペースを含むAzureサブスクリプションをお持ちです。
Microsoft Entra ID監査ログ用のワークブックを作成し、カスタマイズする必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



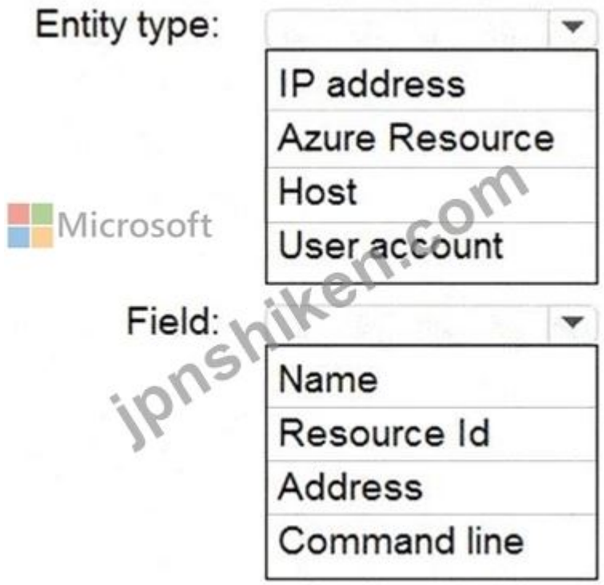
正解:



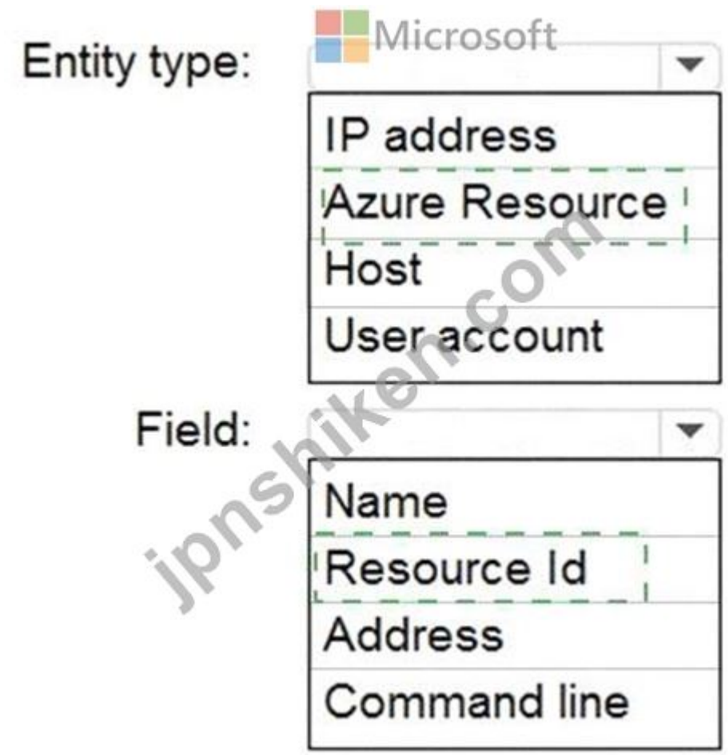
Explanation:



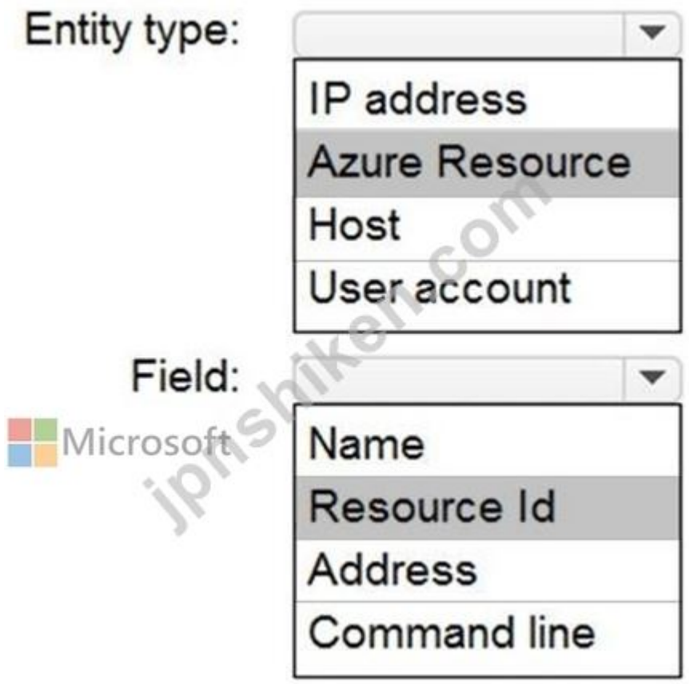
質問: **99**
アプリケーション開発中に複数のAzure Functionsアプリからアクセスされるストレージアカウントをお持ちです。
ストレージアカウントに関するAzure Defenderのアラートを非表示にする必要があります。
抑制ルールでは、どのエンティティタイプとフィールドを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



When configuring suppression rules in Microsoft Defender for Cloud (previously Azure Security Center), you define the specific entity type and field values to suppress recurring or expected alerts. In this scenario, you want to hide Azure Defender alerts for a specific Azure Storage account that is being accessed during application development.
In Defender for Cloud, each protected asset (such as a virtual mach ine, SQL database, or storage account) is represented as an Azure Resource . Therefore, to suppress alerts for that storage account, you must target the Azure Resource entity type.
The unique identifier used to target an exact Azure resource in suppression conditions is its Resource Id , which follows the format:
/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/{resourceProvider}/{resourceName}
By specifying Entity type = Azure Resource and Field = Resource Id , the suppression rule ensures that only alerts generated from that specific storage account are hidden.
Other entity types such as IP address , Host , or User account do not apply to Azure Storage alerts.
Likewise, fields like Address , Command line , or Name are not used for reso urce-based suppression.
Final Answer:
* Entity type: Azure Resource
* Field: Resource Id

質問**: 100**
サポートされているすべてのリソースの種類に対して Azure Defender が有効になっている Azure サブスクリプションがある。
サードパーティのセキュリティ情報およびイベント管理 (SIEM) ソリューションから高重大度アラートを取得できるようにするには、高重大度アラートの継続的なエクスポートを構成する必要があります。
アラートをどのサービスにエクスポートする必要がありますか?
A. Azure Cosmos DB
B. Azure Event Grid
C. Azure Event Hubs
D. Azure データ レイク
正解**: (**正解を表示します**)**
According to Microsoft Defender for Cloud documentation, continuous export allows you to stream security alerts and recommendations to other monitoring or SIEM systems. When exporting alerts in real time, Azure Event Hubs is the supported mechanism. Event Hubs provides a scalable data-streaming platform that can feed events into third-party SIEM tools such as Splunk, IBM QRadar, or ArcSight.
Microsoft states: "To enable real-time streaming of security alerts or recommendations, configure Continuous Export to Azure Event Hubs. From there, your external SIEM or event processing solution can consume the data." The other options serve different purposes:
* Azure Cosmos DB is a NoSQL database, not used for alert streaming.
* Azure Event Grid is for reactive event-driven automation but not intended for continuous log export.
* Azure Data Lake is for large-scale storage and analytics, not streaming.
Thus, exporting Defender alerts to Azure Event Hubs is the correct and supported configuration for continuous export to third-party SIEM solutions.

質問**: 101**
あなたはAzureサブスクリプションをお持ちです。
以下の要件を満たすためには、権限を委任する必要があります。
* Microsoft Defender for Cloud の高度な機能を有効化および無効化します。
* リソースにセキュリティに関する推奨事項を適用する。
解決策は、最小権限の原則に基づかなければならない。
各要件に対して、どの Microsoft Defender for Cloud ロールを使用すべきでしょうか？回答するには、適切なロールを該当する要件にドラッグしてください。各ロールは、1 回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注：正解ごとに1ポイントが加算されます。

正解:

Explanation:

Enable and disable advanced featu res of Microsoft Defender for Cloud: Subscription Owner

* Apply security recommendations to a resource: Security Admin

質問: **102**

ゲストユーザー「User1」とMicrosoft Sentinelワークスペース「workspace1」を含むAzureサブスクリプションをお持ちです。

User1がworkspace1でMicrosoft Sentinelのインシデントをトリアージできるようにする必要があります。このソリューションは、最小権限の原則に基づいている必要があります。

User1にはどの役割を割り当てるべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

正解:

Explanation:

In Microsoft Sentinel, incident management and investigation permissions are controlled through Sentinel- specific Azure roles . To allow a user (including a guest user) to triage incidents - meaning they can view, assign, and update incident statuses , but not modify analytics rules or automation logic - the correct Azure role is Microsoft Sentinel Responder .

Here's the breakdown:

1# # Azure role # Microsoft Sentinel Responder

* The Sentinel Responder role grants permissions to view incidents, update incident status, assign incidents, and run playbooks on incidents.
* It follows the principle of least privilege by limiting access to only incident response and not allowing rule creation, workbook management, or data connector configuration.
* The Sentinel Contributor role, on the other hand, provides broader permissions (including modifying analytic rules), which exceeds the requirement of "triaging incidents."
* Therefore, Microsoft Sentinel Responder is the correct and least-privilege Azure role.

2# # Azure AD role # Directory readers

* To investigate and triage incidents effectively, Sentinel users must be able to resolve user identities (such as usernames, group membership, and object IDs) within Microsoft Entra ID (Azure AD).
* The Directory Readers role provides read-only access to directory data, allowing the user to view identities but not modify them.
* This minimal permission satisfies Sentinel's identity lookup needs without elevating the user to a global administrative or global reader role.

Final Answers:

* Azure role: Microsoft Sentinel Responder
* Azure AD role: Directory readers

質問**: 103**

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. ログ分析トラブルシューティングツールを実行します。
B. 実行可能ファイルをコピーし、ファイル名を ASC_AlerTest_662jf10N,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**)**
The supported way to simulate a host-based alert for Microsoft Defender for Cloud / Azure Security Center is to create and run a benign executable that uses the well-known test filename pattern (commonly shown as ASC_AlertTest_...). Defender for Cloud's alert-validation guidance and simulators describe two supported approaches: (1) use the built-in alert simulator (API) to inject simulated alerts, and (2) exercise host detections by placing/running a specially-named test executable on the target machine so Defender's sensors recognize it and surface a security alert. Creating a copy of any harmless executable (for example, calc.exe) and renaming it to the test filename (the ASC_AlertTest pattern used in Microsoft guidance) is the minimal first step to produce a Defender-for-Cloud alert for validation. This approach requires the Log Analytics / MMA agent or Defender sensor already present on the VM so the telemetry reaches Defender for Cloud.
Why the other options are incorrect: an agent troubleshooting tool or changing MMA settings doesn't directly trigger a detection; the MMASetup -foo argument is not used for alert simulation; and a watchlist is just reference data (it won't generate alerts). For automated, programmatic simulations you can also call Defender for Cloud's Simulate Alerts API, but the quickest on-host validation with minimal administration is to copy
/rename an executable to the ASC_AlertTest filename and run it so Defender generates the expected alert.
Note: Microsoft documentation also recommends using the Defender-for-Cloud alert simulator (REST/API) for bulk or scripted simulations; both methods assume the Defender sensors/agents are installed and reporting.

質問: **104**
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: **(**正解を表示します**)**
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: **105**
Microsoft Defender for Endpoint Plan 2 を使用する Microsoft 365 サブスクリプションがあり、500 台の Windows デバイスが含まれています。Microsoft Defender XDR のカスタム欺瞞ルールを作成する予定です。このルールが特定の 10 台のデバイスにのみ適用されるようにする必要があります。最初に何をすべきですか？
A. 各デバイスの IP アドレスをルールのダミー アカウントとホストのリストに追加します。

B. デバイスをグループに追加します。
C. ルールにカスタムルアーを追加します。
D. デバイスにタグを割り当てる
正解: **(**正解を表示します**)**
Custom deception rules in Defender XDR/Defender for Endpoint can be targeted by scope (e.g., device tags
/device groups). To apply a rule only to a specific subset (10 out of 500), first tag those devices, then target the rule to that tag (or a device group that uses that tag).

質問: **106**
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: クエリからライブストリームを作成します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**
A livestream in Microsoft Sentinel is used for real-time query monitoring , allowing analysts to see new events that match a query as they occur. However, a livestream does not create alerts or incidents automatically .
To generate an incident when a specific condition (like a sign-in from a malicious IP address) occurs, you must create a scheduled analytics rule that runs a KQL query on a defined interval (e.g., every 5 or 10 minutes) and triggers an alert when matches are found.
Microsoft documentation clarifies:
"Livestream is an analyst tool for hunting in real time. It does not generate alerts or incidents. To generate incidents automatically, create an analytics rule using a scheduled query." Therefore, creating a livestream does not meet the requirement to automatically create incidents.
Correct answer: B. No

質問: **107**
組織内の他のユーザーがサインインに使用したことのない場所からユーザーがサインインしようとした場合、セキュリティ警告を受信する必要があります。
どの異常検出ポリシーを使用する必要がありますか?
A. 不可能な旅行
B. 匿名 IP アドレスからのアクティビティ
C. 頻度が低い国からのアクティビティ
D. マルウェアの検出

正解: (正解を表示します)
Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

質問: **108**
Microsoft Sentinelワークスペースをお持ちです。
過去3時間以内に複数の国から正常にサインインしたユーザーを特定するKQL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ポイント獲得できます。

正解:

Explanation:

Below is the completed KQL that meets the requirement (successful sign-ins from multiple countries in the last 3 hours), using the ASIM authent ication schema commonly used in Microsoft Sentinel:

let timeframe = ago(3h);

let threshold = 5;

imAuthentication

| where TimeGenerated > timeframe

| where EventType == " Logon " and EventResult == " Success "

| where isnotempty(SrcGeoCountry)

| summarize

StartTime = min(TimeGenerated),

EndTime = max(TimeGenerated),

Vendors = make_set(EventVendor),

Products = make_set(EventProduct),

NumOfCountries = dcount(SrcGeoCountry)

by TargetUserId, TargetUserPrincipalName, TargetUserType

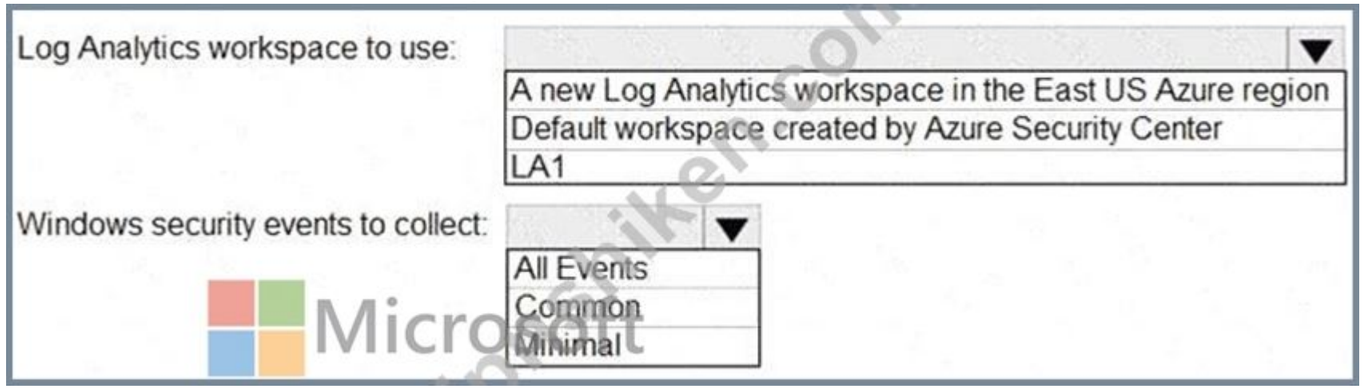
| where NumOfCountries > threshold

* Blade/source: imAuthentication (ASIM parser) normalizes authentication data across sources in Sentinel, letting you query sign-ins consistently.

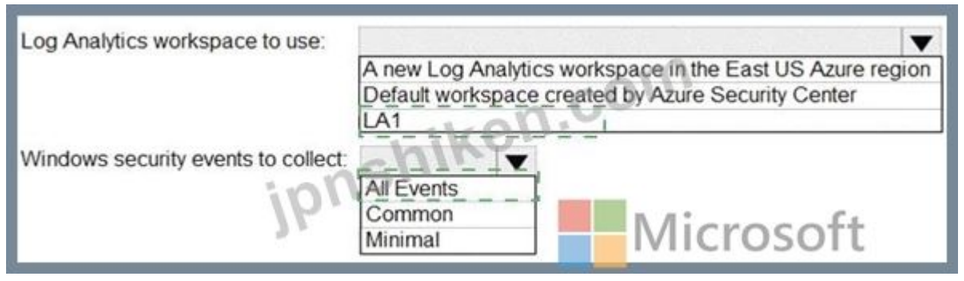
* Filters: EventType == " Logon " and EventResult == " Success " restrict to successful l ogons.

* Geo dimension: SrcGeoCountry is the normalized source country field for the sign-in.
* Logic: We look back 3 hours , count distinct countries per user with dcount(SrcGeoCountry) , and keep only users exceeding a chosen threshold (e.g., > 5).
This delive rs exactly "successful sign-ins from multiple countries during the last three hours," ready for use in a hunting query or to form a scheduled analytics rule.

質問: **109**
Azure Defenderの要件とビジネス要件を満たすためには、Azure Defenderを実装する必要があります。
解答には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:
Log Analytics workspace to use: LA1
Windo ws security events to collect: All Events
To meet the Azure Defender (Microsoft Defender for Cloud) requirement that all servers send logs to the same Log Analytics workspace , you should select the existing workspace LA1 . Defender for Cloud best practic es recommend centralizing data in a single workspace for unified analytics, incident correlation, and cost control. Using the "Default workspace created by Azure Security Center" or creating a new workspace would fragment telemetry, complicate management, and contradict the stated requirement and the business goal to minimize costs (multiple workspaces can increase ingestion/retention overhead and complicate RBAC and automation).
For Windows hosts, Defender for Cloud's Data collection setting controls the l evel of Windows Security Events collected: Minimal , Common , or All Events . The business requirement calls for logs that provide a full audit trail of user activities . In Microsoft guidance, All Events is the level intended for comprehensive auditing (inclu ding logon/logoff, account changes, privilege use, process creation, object access, and other advanced categories). Therefore, to satisfy the "full audit trail" requirement and ensure complete visibility for investigations and Sentinel analytics, choose Al l Events .
In summary: centralize on LA1 (single workspace) and collect All Events to achieve both operational and compliance objectives with Defender for Cloud and Sentinel.

質問: **110**
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、500 台の Windows デバイスが含まれています。インシデント調査の一環として、以下のマルウェアの疑いのあるファイルを特定しました。

* システム
* PDF
* docx
* xlsx

ユーザーがデバイスにファイルをダウンロードできないようにするには、インジケータハッシュを作成する必要があります。インジケータハッシュを使用してブロックできるファイルはどれですか？

A. ファイル1.sysのみ
B. ファイル1.sysとファイル3.docxのみ
C. File1.sys、File3.docx、およびFile4jclsxのみ
D. ファイル2.pdf。ファイル3.docxrとファイル4.xlsxのみ
E. File1.sys、File2.pdf、File3.dooc、およびFile4.xlsx

正解: **(**正解を表示します**)**

In Microsoft Defender for Endpoint (Plan 2), you can use indicator file hashes (IoC file hashes) to block files f rom executing or being downloaded. When you create a file hash indicator, you specify the exact file hash (for example, SHA-256 or MD5) and choose actions such as "block" or "remediate." However, an important detail is that file hash indicators are applied to specific files -that is, for a given executable or file content. You cannot use a hash indicator to block all files of a certain extension generically.

If a given file has a different hash, it will not be blocked unless you add its specific hash. Becaus e the question says you found suspected malware files sys , pdf , docx , xlsx , and you need to block users from downloading those files, only those files for which you can compute and apply a specific hash indicator can be blocked. The question implies you ca n create indicator hashes for each of those file names (assuming each has a unique hash).

Thus you can block all four (File1.sys, File2.pdf, File3.docx, File4.xlsx) by adding each as an indicator hash.

The choice E lists all four. That is consistent with M icrosoft's statements that "you can create indicators that define detection, prevention, or exclusion of entities," and file hash indicators specifically apply to those files.

Microsoft Learn+3Microsoft Learn+3Microsoft Learn+3

Options that exclude some file types (e.g. only blocking sys and docx but not pdf or xlsx) would leave gaps, which doesn't satisfy the requirement of blocking all those suspected files. Hence E is the correct answer.

質問**: 111**

Microsoft Defender for Cloud の要件とビジネス要件を満たすために、Group1 と Group2 にロールベースのアクセス制御 (RBAQ ロール) を割り当てる必要があります。各グループにはどのロールを割り当てるべきですか？

回答するには、回答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:

In Microsoft Defender for Cloud , Role-Based Access Control (RBAC) is used to ensure that users and groups have only the permissions required to perfor m their specific security or management tasks. Microsoft provides several built-in roles designed specifically for Defender for Cloud operations.

* Security Admin: This role provides full management permissions for security policies, recommendations, and alerts within Defender for Cloud. A Security Admin can configure policies, suppress or dismiss alerts, enable or disable Defender plans, and manage settings at the subscription or management group level. According to Microsoft documentation, the Security A dmin role "has all permissions of the Security Reader role plus the ability to update security policies and dismiss alerts and recommendations." Therefore, Group1 , which likely needs administrative control to manage and remediate findings, should be assign ed Security Admin .

* Security Assessment Contributor: This role is more limited and focuses on providing access for security posture assessment without granting the ability to change or modify configurations. The Security Assessment Contributor role allows v iewing security recommendations and assessment data but not altering Defender for Cloud configurations or dismissing alerts. This makes it ideal for compliance or audit groups who need read and assess access. Hence, Group2 should be assigned Security Assessment Contributor .
These assignments ensure the right balance between operational control (Group1) and read-only assessment or compliance duties (Group2), aligning with Microsoft's least-privilege and separation-of-duties best practices.
Final Answe r:
* Group1 # Security Admin
* Group2 # Security Assessment Contributor

質問**: 112**
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. [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。
B. [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。
C. [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。
D. [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。
E. [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。
F. [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。
正解**: B,F (**コメントを発表する**)**

質問**: 113**
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**)**
Explanation (concise): To send a Microsoft Teams message when a suspicious sign-in is detected, create a playbook (Logic App) that posts to Teams (A) and associate the playbook so it runs when the corresponding alert/incident is created (B)-typically via an automation rule or by attaching the playbook to the analytics rule/incident. Entity behavior analytics, workbooks, or Fusion aren't required for sending Teams notifications.

質問**: 114**
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。
Microsoft Defender XDR を使用する Microsoft 365 サブスクリプションをお持ちの場合、攻撃者がデバイス上で以下の操作を実行したことが判明しました。

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. 分析
B. レジストリ
C. 修復する
D. スキャン
正解: **B (**コメントを発表する**)**
In a Microsoft Defender for Endpoint live response session , the registry command is used to interact with and modify the Windows Registry remotely. Since the attac ker changed a registry-based antivirus exclusion path, you can undo that modification directly using the registry command.
The registry command allows you to view, add, delete, or modify keys and values in the registry during a live response session.
* analy ze is used to inspect files.
* remediate is used to remove threats detected by Defender.
* scan is used to trigger antivirus scans. Therefore, to undo a registry change , the correct command is registry .
# Answer: B. registry

質問**: 115**
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
インシデントページから直接、侵害指標(LoC)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**)**
I n Microsoft Sentinel , during incident investigation, you can label certain entities directly from the incident page as Indicators of Compromise (IOCs) . According to Microsoft Sentinel's entity behavior and investigation documentation, entities such as IP a ddresses , URLs , file hashes , and domains can be directly marked as IOCs because they represent observable threat indicators that can be tracked across the environment.
While entities like User accounts , Hosts , and Malware names are part of incident context , they are not directly taggable as IOCs from the incident page because Sentinel expects IOCs to represent specific, traceable, external threat artifacts (e.g., IPs, domains, or file hashes).
Therefore, from the list provided - Host, IP address, User account, and Malware name - only the IP address entity can be directly labeled as an IOC from within the incident interface in Sentinel.
Answer: D. IP address

質問**: 116**
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: **(**正解を表示します**)**
Applying "quick fix" remediations from Azure Defender (Microsoft Defender for Cloud) changes the underlying resources (VMs). Beyond the Security Admin role (which grants security policy/manage permissions), the user needs write permissions on the target resources. To follow least privilege, grant Contributor on RG1 (the resource group containing the 100 VMs) so SecAdmin1 can remediate only those resources-rather than the entire subscription (over-privilege) or Owner (unnecessary). Security Reader is read-only and cannot apply fixes.

質問: **117**
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 ワークスペースでは、以下のプラグインが使用されています。
* マイクロソフトが参入
* Microsoft Defender XDR
Microsoft Defender ポータルから、Copilot for Security を使用して報告されたインシデントを調査します。調査には、Microsoft Entra ID Protection からの情報が含まれるプロンプトブックを実行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 ポータルからインシデント レポートを作成します。
B. Microsoft Defender ポータルから、高度なハンティングクエリを作成します。
C. Microsoft Sentinel で調査を開始します。
D. Copilot for Security スタンドアロン版で調査を開始します。
正解: **(**正解を表示します**)**

質問: **118**
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。このサブスクリプションには、Microsoft Defender for Endpoint にオンボーディングされた 500 台の Windows 11 デバイスが含まれています。デバイス上の Administrators グループのメンバーシップに不正な変更が加えられていることを発見しました。次の要件を満たすソリューションを構成する必要があります。
* 1時間ごとに、各エンドポイントの管理者グループメンバーシップを確認してください。
* 管理者グループのメンバーシップの変更が検出されたら、Microsoft Defender XDR でインシデントを作成します。
最初に何を作るべきでしょうか？
A. 高度なハンティングクエリ
B. デバイスグループ
C. アラート調整ルール
D. 検出ルール
正解: **(**正解を表示します**)**

質問: **119**
あなたはMicrosoft Exchange Onlineを使用するMicrosoft 365 E5サブスクリプションを所有しています。以下の表に示す不審なメールを特定しました。

Name	From	Subject	Date 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 ポータルでは、次の表に示す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)`

以下の各設問について、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点が加算されます。

Statements	Yes	No
Search1 will include Email1.	○	○
Search2 will include Email2.	○	○
Search3 will include Email3.	○	○

正解:

Statements	Yes	No
Search1 will include Email1.	○	○
Search2 will include Email2.	○	○
Search3 will include Email3.	○	○

Explanation:

質問: **120**
Microsoft Sentinel を使用する Azure サブスクリプションがあります。
インシデントに対応し、Microsoft Sentinel によって検出されたセキュリティの脅威を修復するために必要な管理労力を最小限に抑える必要があります。
どの 2 つの機能を使用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. Microsoft Sentinel ブックマーク
B. Azure Automation Runbook
C. Microsoft Sentinel 自動化ルール
D. Microsoft Sentinel プレイブック
E. Azure Functions アプリ
正解: **(**正解を表示します**)**
To minimize administrative effort in responding to incidents and remediating security threats in Microsoft Sentinel, you should use the platform's built-in automation and orchestration capabilities - specifically Automation Rules and Playbooks.
* Microsoft Sentinel Automation Rules (Option C):
* Automation rules in Sentinel allow you to automate incident management tasks such as assigning owners, changing severity, tagging, or automatically running playbooks when an incident or alert is created.
* They help standardize responses across similar alerts, significantly reducing manual intervention.
* Microsoft documentation states:
"Automation rules simplify the management of playbook triggers and incident handling by allowing you to define actions that automatically occur when incidents are created or updated."
* Microsoft Sentinel Playbooks (Option D):
* Playbooks are Logic App-based workflows that automate responses to security alerts or incidents.
* They can perform remediation actions such as disabling compromised accounts, isolating infected devices, blocking IP addresses, or sending notifications to SOC teams.
* You can link playbooks directly to analytics rules or call them through automation rules for end- to-end automation.
Incorrect Options:
* A. Bookmarks are used for hunting investigations, not for automation or remediation.
* B. Azure Automation runbooks can be used for specific administrative scripts but require more manual setup and integration - not the most efficient choice for Sentinel's automated workflows.
* E. Azure Functions apps are custom code execution environments; while powerful, they are not the primary tool for Sentinel's automated response.

質問: **121**

Microsoft Defender XDR を使用する Microsoft 365 B5 サブスクリプションをお持ちです。インシデントを調査しています。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。インシデント ページでは何が使用できますか?

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)
On the Microsoft Defender (Microsoft 365 Defender) Incident page, investigators need a complete view of what actions were taken and when. The UI provides multiple panes to support that: the Tasks area (lists manual and automated investigation/remediation tasks assigned to the incident), the Activity log (chronological audit of user and system actions taken on the incident such as assignments, status changes, playbook runs and remediation actions), and the Alert timeline (a timeline view showing the alerts that make up the incident and the sequence of alerts and related detections/events). Microsoft's investigation guidance describes all three surfaces as part of the incident investigation workflow: tasks capture work items and owner actions, the activity log provides an auditable history of actions and changes, and the alert timeline visualizes the alert and event sequence that drove the incident. Because the question asks specifically for reviewing the incident tasks that were performed , the incident page exposes the tasks list and also the activity log and alert timeline so you can see when tasks ran, who ran them, what automated playbooks or remediation executed, and how those tasks related to the underlying alerts. For full incident forensics and auditability you use Tasks
+ Activity log + Alert timeline .

質問: **122**
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 のデバイス管理からのオンボーディング設定
B. クラウドアプリセキュリティの異常検知ポリシー
C. Microsoft Defender セキュリティ センターの設定の高度な機能
D. クラウドアプリセキュリティのクラウド検出設定
正解: (正解を表示します)
To block unsanctioned cloud apps on Windows 10 endpoints with Microsoft Defender for Endpoint and Microsoft Defender for Cloud Apps (formerly Cloud App Security), you must enable and configure the product integration on both sides. First, in Microsoft Defender Security Center # Settings # Advanced features , turn on the Microsoft Defender for Cloud Apps integration (and ensure network protection prerequisites are met). This allows Defender for Endpoint to receive the unsanctioned app list and enforce endpoint-based blocking when users on CLIENT1 attempt to access those apps via the browser or client.
Second, in Defender for Cloud Apps # Settings # Cloud Discovery , configure the Microsoft Defender for Endpoint integration and enable Block unsanctioned apps . In Cloud Discovery, apps are discovered, assessed, and can be tagged as Unsanctioned . Once the MDE integration is enabled, that tag is exported to endpoints, which then enforce blocking based on the tenant's app catalog and policies.
Options A (Onboarding settings) are for enrolling devices and do not control app blocking behavior. B (Anomaly detection policies) govern behavioral detections (e.g., impossible travel, anonymous IP) and are unrelated to endpoint enforcement of app access. Therefore, the two configurations you must modify to meet the require ment "block unsanctioned apps on Windows 10 computers by using Microsoft Defender for Endpoint" are C. Advanced features in Microsoft Defender Security Center and D. Cloud Discovery settings in Cloud App Security .

質問: **123**
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製品がインストールされ、Microsoft Defender Antivirus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アーティファクトからデバイスを保護する必要があります。解決策：自動調査および対応(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)
Automated Investigation and Response (AIR) automates investigation and remediation actions for alerts that Defender already detects: it triages alerts, runs investigation playbooks, and can execute remediation (quarantine files, terminate processes, remove persistence) based on the investigation outcome. AIR is powerful for reducing analyst load and quickly remediating detected threats. However, AIR only runs in response to detections/alerts it receives-if the third-party AV completely misses an artifact and no EDR
/behavioral detection generates an alert, AIR will not be triggered. In contrast, EDR in block mode is specifically built to catch post-breach detections that the primary AV missed and to remediate them. Therefore, enabling AIR alone does not guarantee protection from artifacts missed by the third-party antivirus; AIR helps remediate once a detection exists but does not itself create the missed detection coverage that EDR in block mode provides.

質問: **124**
Microsoft Defender for Cloud が有効になっている Microsoft サブスクリプションをお持ちの場合、次の表に示す Azure ロジック アプリを構成します。

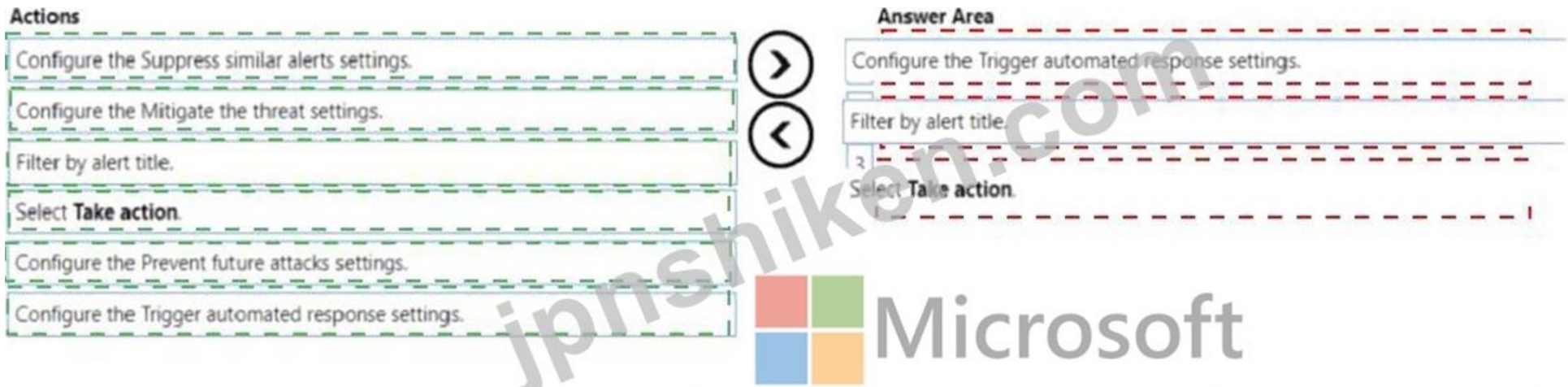
Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

不審なプロセスが実行されたというアラートがトリガーされた場合に実行される自動アクションを設定する必要があります。
解決策は、管理上の負担を最小限に抑えるものでなければならない。
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。

Actions
- Configure the Suppress similar alerts settings.
- Configure the Mitigate the threat settings.
- Filter by alert title.
- Select **Take action**.
- Configure the Prevent future attacks settings.
- Configure the Trigger automated response settings.

Answer Area
1.
2.
3.

正解:



Explanation:
Select Take action.
Configure the Trigger automated response settings.
Filter by alert title.
In Microsoft Defender for Cloud, automatic responses to alerts are implemented through Take action # Trigger automated response , which creates or binds a workflow automation to a Logic App. For an alert such as "Suspicious process executed" , the least-effort approach is to start from the alert experience and attach the prebuilt Logic App that uses the "When a Defender for Cloud alert is created or triggered" trigger (your LogicApp2). The documented flow is: open the alert and choose Take action ; within that blade, select Trigger automated response to connect a Logic App; then scope the automation by setting conditions/filters , including Alert title , so it only runs when the specific alert ("Suspicious process executed") is generated. This maps exactly to the three steps above.
Other panes under Take action - Mitigate the threat and Prevent future attacks -provide manual guidance or recommend hardening steps and are not used to bind a Logic App. Similarly, Suppress similar alerts is for tuning noise, not for launching automations. Because you already have LogicApp2 with the Defender for Cloud alert trigger, selecting Trigger automated response and filtering by alert title ensures the playbook runs every time that specific alert fires , with minimal administration and without creating additional custom logic.

質問: **125**
あなたは、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 ポータルで、Device1 に対してアラートがトリガーされたことを確認しました。デバイス インベントリ ページから Device1 を隔離します。Device1 にインストールされているプログラムの一覧を取得する必要があります。どうすればよいですか？
A. DeviceTvmInfoGathering 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。
B. ライブレスポンスセッションを開始し、processsコマンドを実行します。
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. 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。
正解: **C (**コメントを発表する**)**
The DeviceTvm SoftwareInventory table in Microsoft Defender XDR advanced hunting contains detailed information about installed applications, software versions, publishers, and installation details across onboarded endpoints. When you need to retrieve a list of installed programs for a specific device (like Device1), this is the correct table to query.
Microsoft documentation describes this table as:
"The DeviceTvmSoftwareInventory table provides a comprehensive inventory of all software discovered on devices, including v ersion and vendor information."
* DeviceTvmInfoGathering contains vulnerability assessment and scan status details, not software lists.
* DeviceProcessEvents captures process execution data (runtime events).
* Live response processes command lists currently running processes, not all installed software.
# Correct Answer: C. DeviceTvmSoftwareInventory

質問: **126**

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。

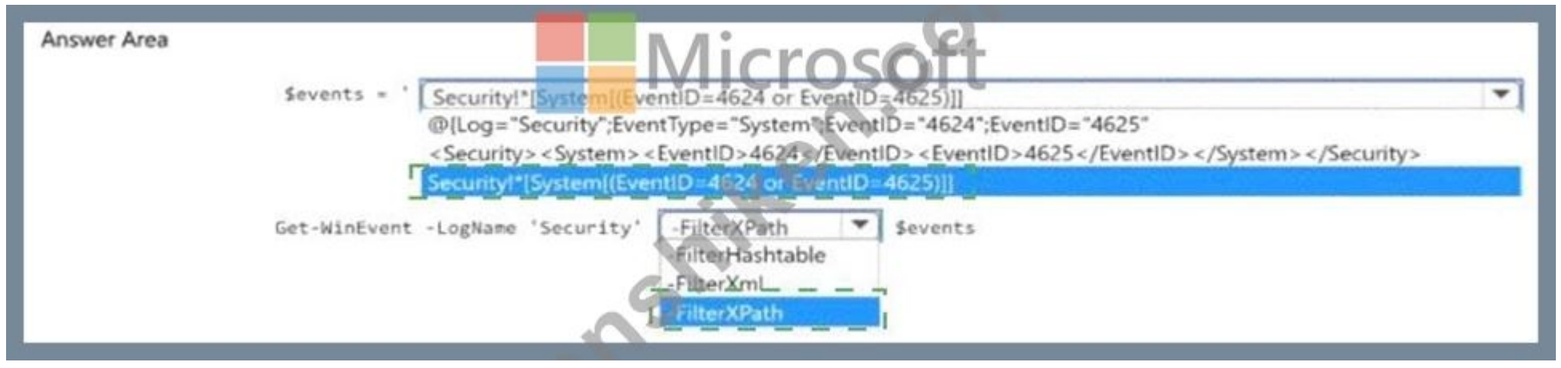
収集するイベントの範囲を、イベント4624と462Sのみに限定する予定です。

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。

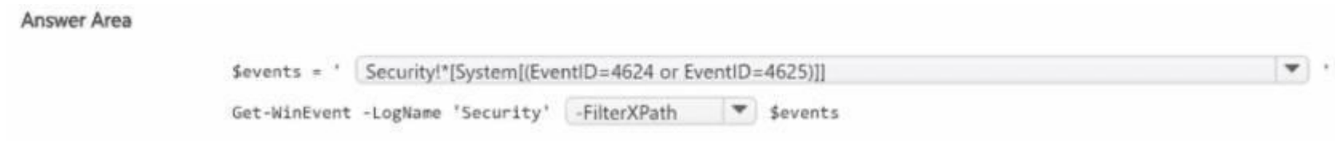
スクリプトをどのように完成させればよいでしょうか？回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

正解:



Explanation:



According to Microsoft Sentinel and Azure Monitor Agent (AMA) documentation, when configuring data collection from Windows Security logs, you can use XPath filtering to limit which event IDs are collected.

This hel ps optimize data ingestion by filtering out unnecessary events.

In this scenario, the requirement is to collect only event IDs 4624 (successful sign-in) and 4625 (failed sign- in) . The PowerShell cmdlet Get-WinEvent supports several filtering methods: -Filt erXPath , -FilterHashtable , and -FilterXml . To test the same XPath syntax used by the connector, you must use - FilterXPath , because this option accepts the same XPath query string format as used in the AMA data collection rule (DCR).

The correct XPath synta x for filtering specific event IDs from the Security log is:

Security!*[System[(EventID=4624 or EventID=4625)]]

This expression instructs the event query to return only events from the Security log whose EventID equals

4624 or 4625.
Finally, to validate th e filter, you run:
Get-WinEvent -LogName ' Security ' -FilterXPath $events
This command executes the filter locally and confirms that the syntax correctly retrieves the intended events.
Therefore, the correct completed script is:
$events = ' Security!*[Syst em[(EventID=4624 or EventID=4625)]] '
Get-WinEvent -LogName ' Security ' -FilterXPath $events

質問: **127**
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**)**
Just-in-time (JIT) VM access and network layer threat detections are features of Microsoft Defender for Cloud (formerly Azure Security Center "Azure Defender" plans). These capabilities are enabled by turning on the relevant Defender plans at the subscription level, which then apply to resources in that subscription.
Workspace- or individual resource-level enablement won't activate JIT or the broad network detections across your estate.

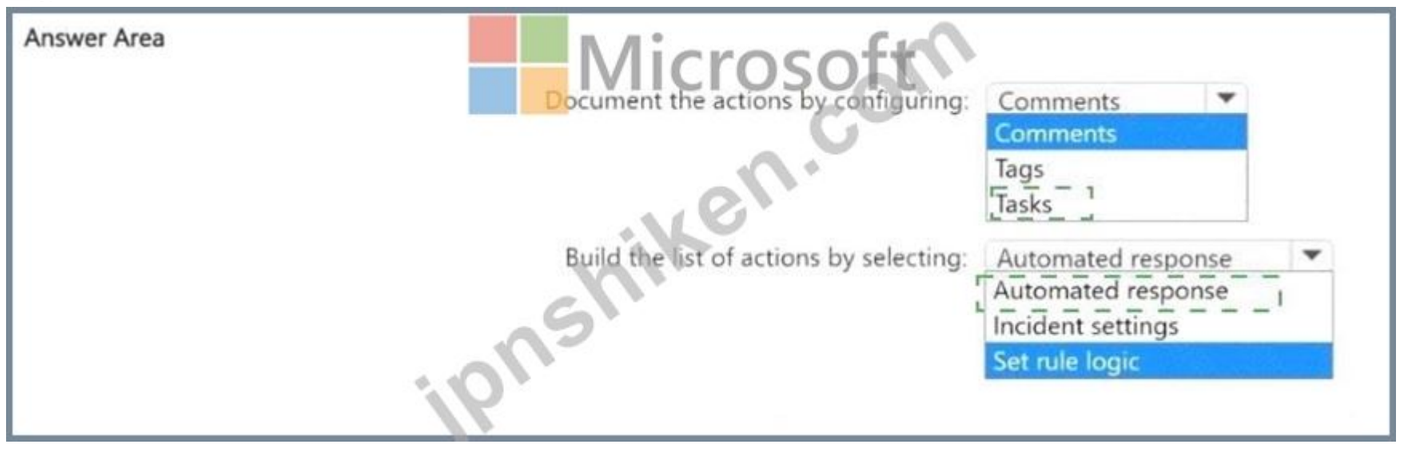
質問: **128**
あなたの会社には、Microsoft Defender for Identity を使用するオンプレミス ネットワークがあります。
企業の Microsoft Secure Score には、安全でない Kerberos 委任に関連するセキュリティ評価が含まれています。
セキュリティ リスクを修正する必要があります。
あなたは何をするべきか？
A. 公開エンティティとしてリストされているコンピューターに Local Administrator Password Solution (LAPS) 拡張機能をインストールします。
B. 公開エンティティとしてリストされているコンピュータ オブジェクトのプロパティを変更します。
C. 公開エンティティとしてリストされているコンピューター上のレガシー プロトコルを無効にします。
D. 公開エンティティとしてリストされているコンピューターに LDAP 署名を強制します。
正解: **B (**コメントを発表する**)**
To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either ' Trust this computer for delegation to any service ' or ' Trust this computer for delegation to specified services only ' . This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network. Reference: https://docs.microsoft.com/en-us/windows /security/identity-protection/microsoft-defender-for-identity/configure-k erberos-delegation

質問: **129**
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、実行すべき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。ソリューション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。

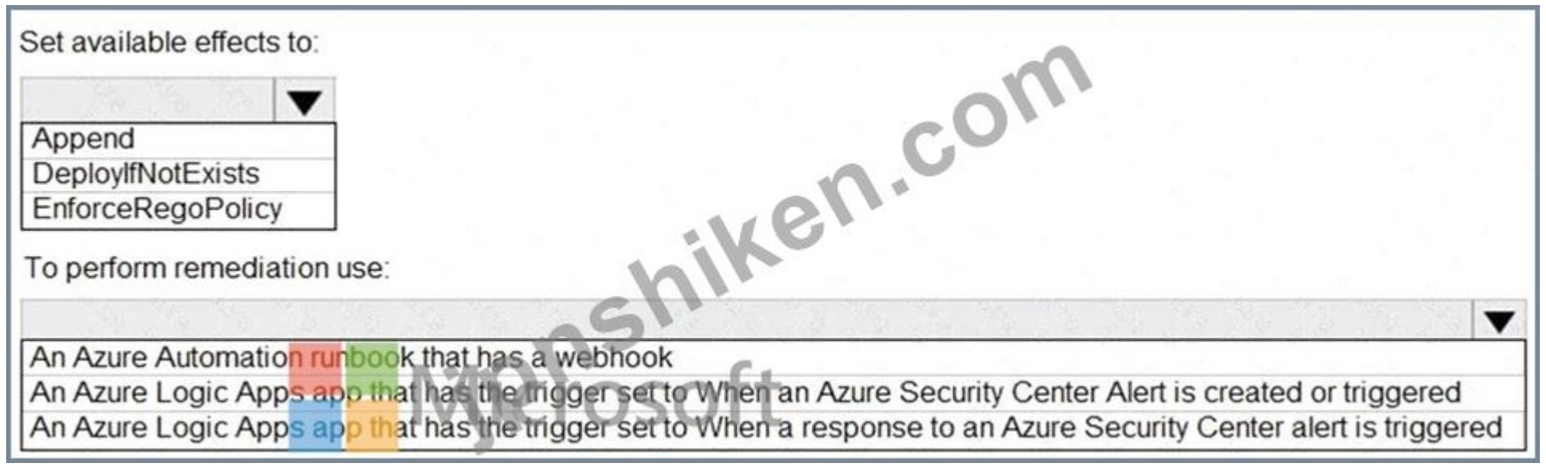
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

Answer Area

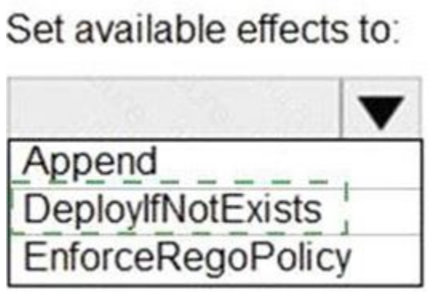
正解:

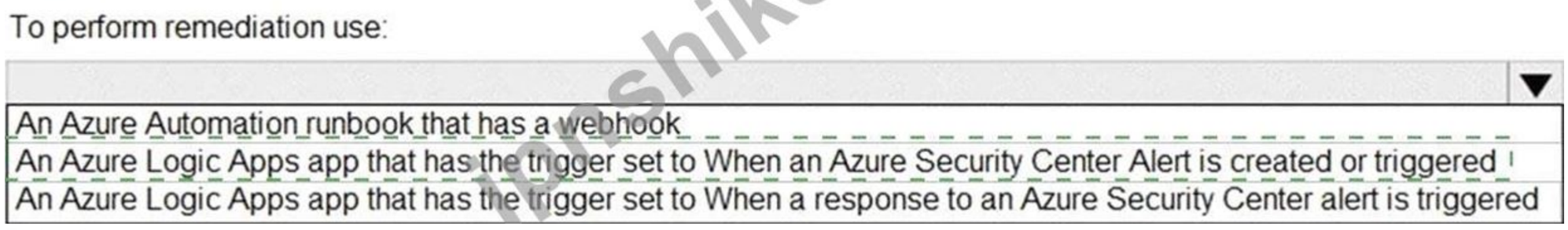


質問: **130**
お客様はAzure Defenderを使用するAzureサブスクリプションをお持ちです。
Azure Security Centerのワークフロー自動化機能を使用して、Azure Defenderの脅威アラートに対応する予定です。
脅威の修復を自動的に実行するAzureポリシーを作成する必要があります。
解答には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

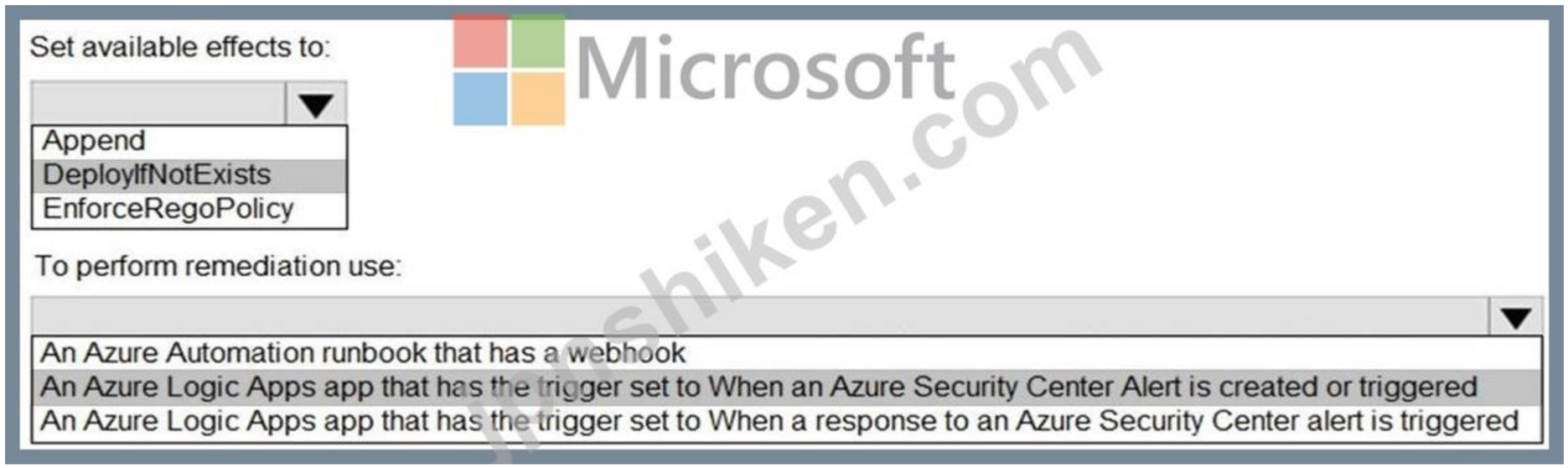


正解:





Explanation:



In Microsoft Defender for Cloud (formerly Azure Security Center) , workflow automation allows you to automatically respond to security alerts and recommendations by triggering remediation actions.
When you create an Azure Policy to enforce automatic remediation based on Defender alerts or recommendations, the effect determines what the policy does when a resource is found noncompliant:
* DeployIfNotExists is the correct effect to use for automatic remediation. This effect automatically deploys a remediation task (such as a Logic App or other automation) when a matching noncompliant resource is detected. It's commonly used in Defender for Cloud to deploy missing security configurations or initiate an automated remediation workflow.
* Append only adds metadata or parameters to resources-it does not enforce or deploy remediation actions.
* EnforceRegoPolicy is used for container compliance with Gatekeeper policies (Kubernetes), not for Defender workflows.
For the automation mechanism:
* An Azure Logic Apps app with the trigger "When an Azure Security Center alert is created or triggered" is the correct choice. This Logic App acts as the workflow automation engine that runs whenever a new alert is raised. It can perform actions such as isolating VMs, disabling users, or notifying SOC teams.
* Using a trigger for "When a response to an Azure Security Center alert is triggered" would only activate after a manual response, not automatically.
* Automation runbooks with webhooks can be used for custom automation, but Defender workflow automation integrates natively with Logic Apps and not directly with runbooks.
# Final answer:
* Set available effects to: DeployIfNotExists
* To perform remediation use: An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered

質問**: 131**
以下のKQLクエリを含むカスタム検出ルールがあります。

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

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

Answer Area

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

正解:

Answer Area

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

Explanation:

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.	○	●

質問: **132**
Microsoft Defender for Cloudを使用するAzureサブスクリプションがあり、RG1という名前のリソースグループが含まれています。RG1内の仮想マシンに対して、ジャストインタイム(JIT)VMアクセス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。
* リクエストの最大時間を2時間に制限してください。
* プロトコルアクセスをリモートデスクトッププロトコル(RDP)のみに制限します。

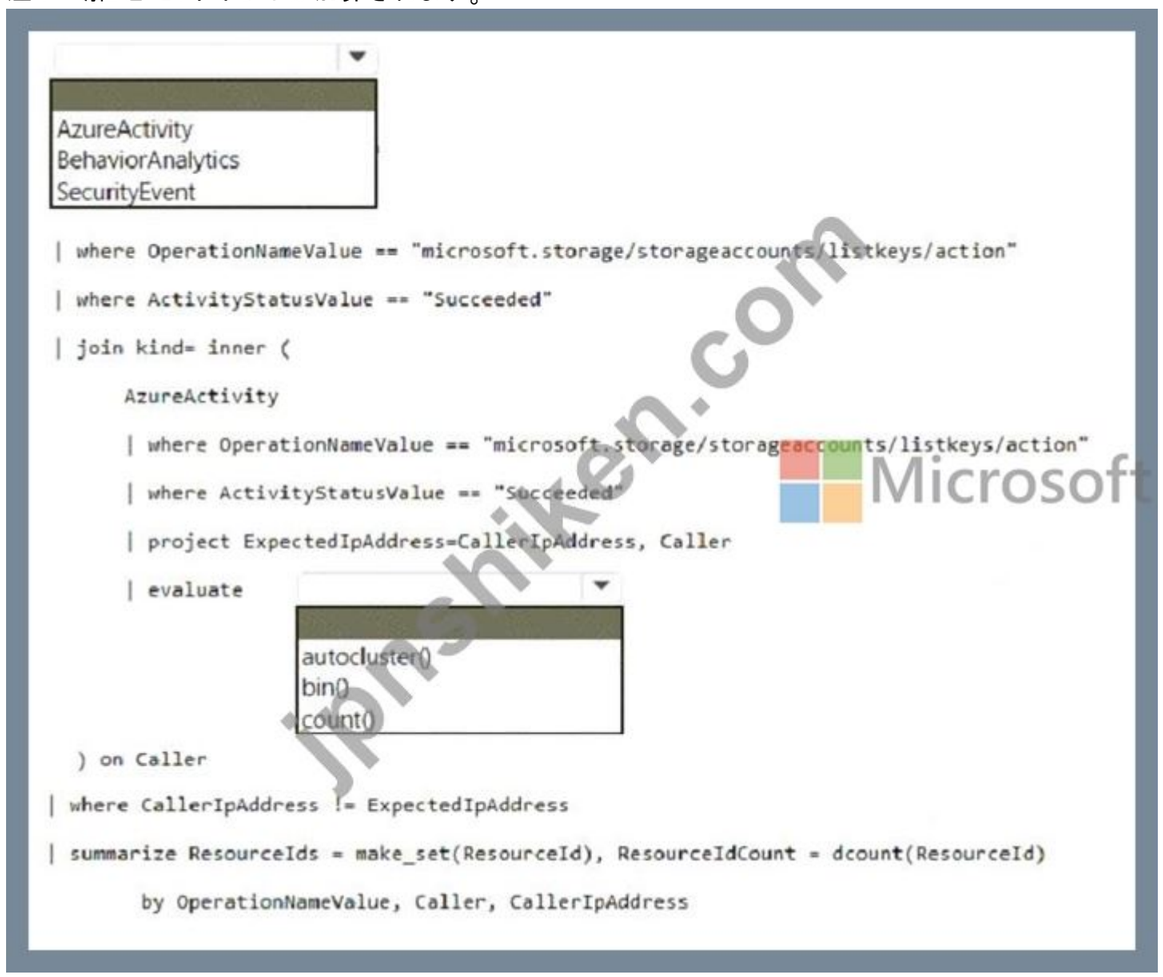
管理業務の手間を最小限に抑える。
何を使うべきでしょうか？
A. Azure AD 特権ID管理 (PIM)
B. Azure Policy
C. アジュールフロントドア
D. アジュールバスティオン
正解: **(**正解を表示します**)**
Just-In-Time (JIT) VM access in Microsoft Defender for Cloud controls inbound traffic to virtual machines, reducing exposure to attacks. Microsoft's guidance allows JIT policies to be centrally configured and applied automatically across a resource group using Azure Policy , which provides the lowest administrative overhead.
To meet the requir ements:
* Limit request time to two hours: Defender for Cloud JIT policy allows defining a maximum allowed access duration per request.
* Limit protocol to RDP only: The JIT configuration can restrict the protocol and port (TCP/3389 for RDP).
* Minimize administrative effort: Azure Policy can automatically enforce this configuration for all VMs in RG1 without manually setting up each VM.
Other options are less suitable:
* A. PIM controls user privileges, not network access.
* C. Azure Front Door handles web application traffic.
* D. Azure Bastion provides secure RDP/SSH via portal but doesn't manage just-in-time network policies.
# Correct Answer: B. Azure Policy

質問: **133**
Microsoft Sentinelの要件を満たすには、どのルール設定を構成すればよいですか？
A. セットルールロジックから、抑制をオフにします。
B. 分析ルールの詳細から、戦術を設定します。
C. セットルールロジックからエンティティをマッピングします。
D. 分析ルールの詳細から、重要度を設定します。
正解: **(**正解を表示します**)**
In Microsoft Sentinel, entity mapping is a critical configuration that ensures detected events and alerts are correctly represented in the investigation graph , incidents , and hunting experiences . The Sentinel requirements in the case study specify:
"Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting." To meet this requirement, the analytic rule must be configured to map entities such as IP address, user, hostname, or URL in the Set rule logic section. This mapping allows the incident and its related alerts to visually associate with those entities, enabling analysts to pivot and investigate in the Sentinel investigation graph.
According to Microsoft Sentinel documentation:
"Entity mapping in analytic rules helps correlate alerts and incidents to specific entities such as accounts, IPs, or hosts, enabling richer investigation experiences and faster triage." Therefore, configuring entity mapping directly under Set rule logic ensures that incidents are enriched with contextual information (for example, the specific IP address), meeting both the functional and investigative requirements.
Final Answer for Question 2: C. From Set rule logic, map the entities.

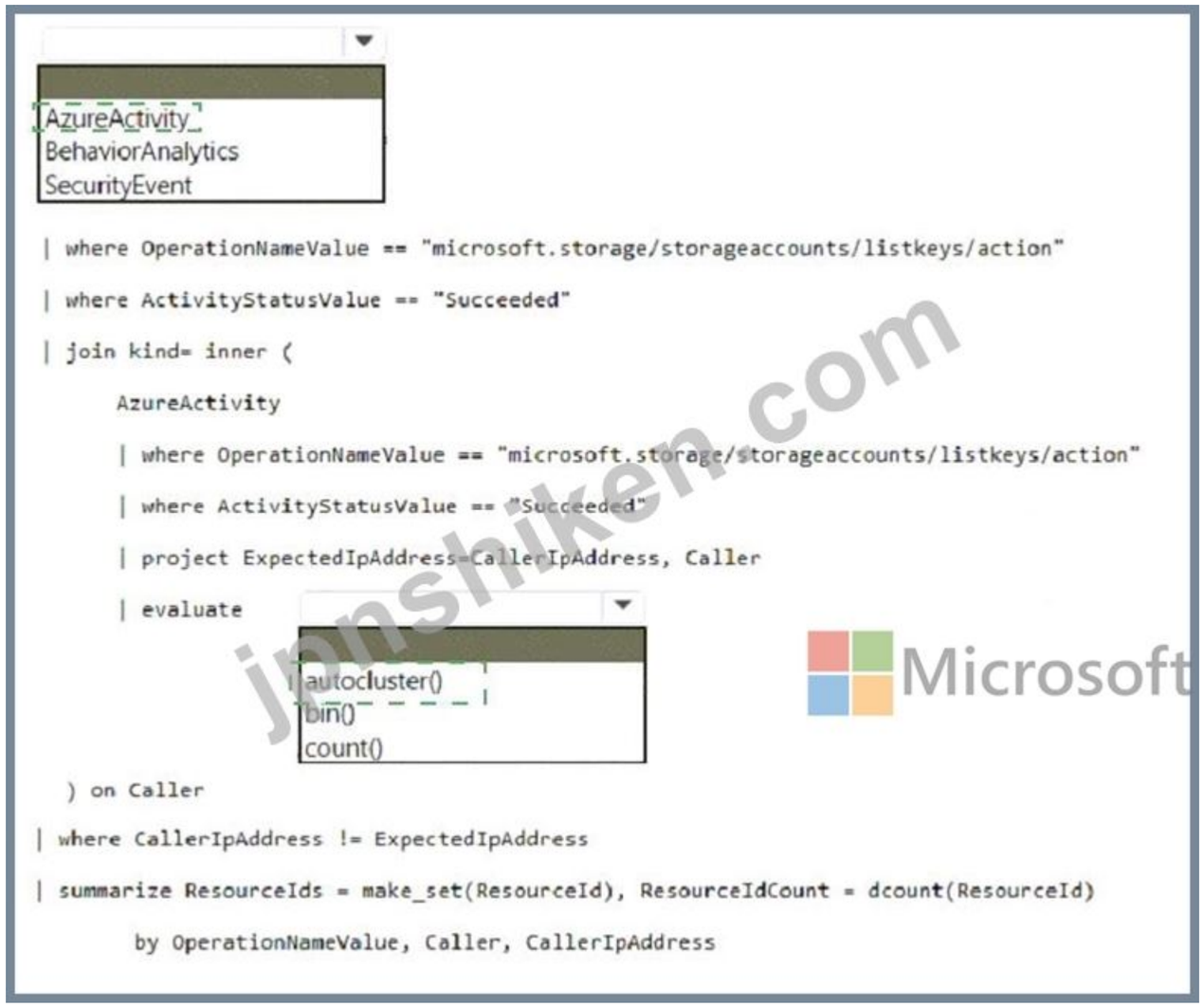
質問: **134**
サードパーティ製のセキュリティ情報およびイベント管理(SIEM)ソリューションを使用して、Microsoft Defender for Cloudのアラートをレビューする予定です。
MITRE ATT & CKの特権昇格戦術の使用を示すアラートを特定する必要があります。
どのJSONキーを検索すればよいですか？

A. インテント
B. 説明
C. 拡張プロパティ
D. エンティティ
正解: (正解を表示します)
Defender for Cloud alerts include a kill chain intent field that maps to MITRE ATT & CK tactics (for example, PrivilegeEscalation , Persistence , CredentialAccess). In the alert JSON this is exposed as intent ; searching that key lets you filter for alerts where the tactic is Privilege Escalation.

質問: **135**
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 Storage アカウントのストレージ キーをリストアップしているユーザーを特定するには、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アップしているユーザーを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:

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: **136**
Microsoft Sentinelの要件を満たすために、どの平均時間メトリックを使用するかを特定する必要があります。どのワークブックを使用すればよいでしょうか？
A. 分析効率
B. セキュリティ運用効率
C. イベントアナライザー
D. 調査結果
正解: (正解を表示します)
Microsoft Sentinel provides built-in workbooks for oper ational insights. To analyze mean time metrics (Mean Time to Acknowledge, Mean Time to Resolve, Mean Time to Mitigate), the correct workbook is Security Operations Efficiency .
According to Microsoft's Sentinel documentation:
"The Security Operations Effici ency workbook helps SOC teams monitor and improve operational performance by showing incident trends and key performance indicators such as mean time to acknowledge (MTTA), mean time to resolve (MTTR), and incident closure rates." Other options:
* Analytics Efficiency - tracks analytic rule performance.
* Event Analyzer - provides event data analysis, not MTTA/MTTR.
* Investigation Insights - focuses on incident investigation details, not SOC metrics.
# Correct workbook: Security Operations Efficiency

質問: **137**
Azure Sentinel ワークスペースがあります。
Azure portal でプレイブックを手動でテストする必要があります。Azure Sentinel のどこからテストを実行できますか?
A. ハンドブック
B. 分析
C. 脅威インテリジェンス

D. インシデント

正解: **D** (コメントを発表する)

In Microsoft Sentinel, playbooks (Logic Apps) that are connected to Sentinel are most commonly run in context of an incident. From the Incidents blade, you select an incident, then choose Actions # Run playbook to trigger a manual test against that specific incident's entities and alert context. This is the recommended way to validate playbook inputs (entities, alert details, incident properties) and permissions end-to-end without changing analytics rules. While the Playbooks blade shows the Logic Apps and their connections, the incident view is where Sentinel exposes manual execution with full security operations context (assignments, comments, evidence), which is what "test a playbook manually in the Azure portal (from Sentinel)" refers to.

質問: **138**

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。

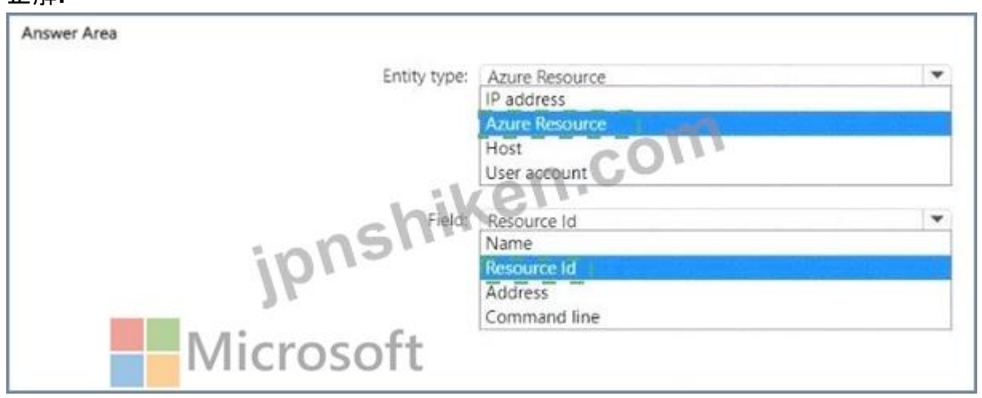
ストレージアカウントに関するMicrosoft Defender for Cloudのアラートを非表示にする必要があります。

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:



Explanation:

In Microsoft Defender for Cloud , suppression rules are used to automatically hide or suppress specific alerts that match defined conditions. These rules are often configured when certain alerts are expected (for example, during development or testing) and do not represent true security risks.

According to Microsoft Defender for Cloud documentation , when creating a suppression rule for a particular Azure resource (like a Storage account), you must select the appropriate entity type and field that uniquely identify that resource.

* The Entity type defines what the suppression condition applies to. To suppress alerts for a specific Azure resource such as a storage account, virtual machine, or function app, the correct selection is Azure Resource .

* The Field defines the attribute used to match that resource. Microsoft's guidance specifies that Resource Id is the unique identifier for every Azure resource within a subscription, formatted as:

* /subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/{resourceProvider}/{resourceType}/{resourceName}

This ensures the suppression rule precisely targets alerts related only to that specific storage account and not others.

Alternative fields like Name , Address , or Command line do not uniquely identify Azure resources in Defender for Cloud. Therefore, they would not provide the necessary precision for suppressing alerts from a specific Azure Storage account.

Final Answers:

* Entity type: Azure Resource

* Field: Resource Id

質問: **139**

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

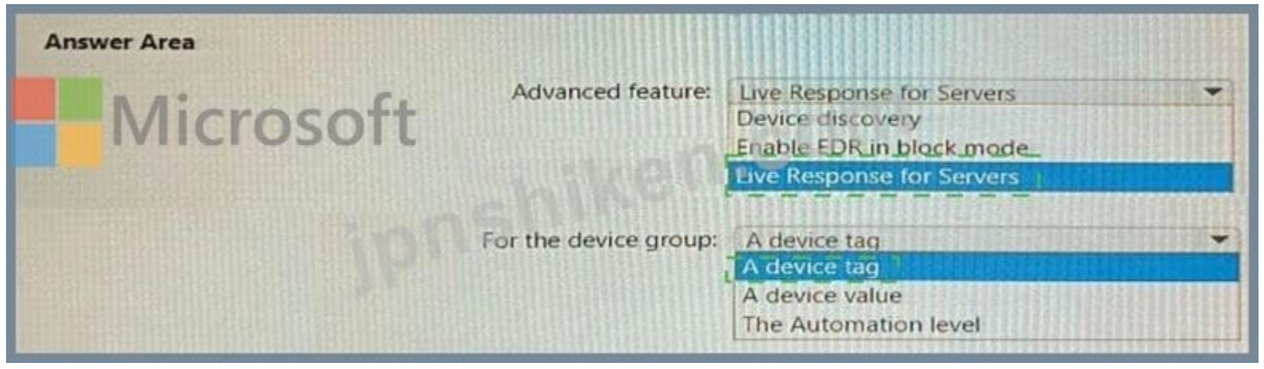
Microsoft を使用して Windows サーバーへのリモート シェル接続を開始できることを確認する必要があります

365 Defenderポータル。

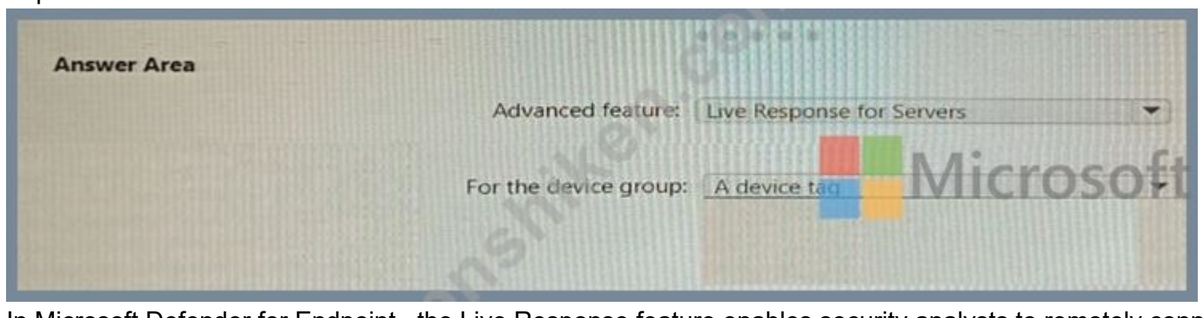
何を設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

正解:



Explanation:



In Microsoft Defender for Endpoint , the Live Response feature enables security analysts to remotely connect to devices (including servers) via a secure shell session directly from the Microsoft 365 D efender portal . This feature allows real-time investigation, evidence collection, and remediation commands without requiring direct network access to the device.

To enable this capability for Windows servers , you must first enable the "Live Response for Se rvers" advanced feature within Defender for Endpoint settings. Microsoft's documentation explicitly states that this setting allows remote shell access to onboarded Windows Server devices, which is disabled by default for security reasons.

Once the advance d feature is enabled, Live Response permissions and functionality are managed at the device group level. Device groups in Defender for Endpoint are typically configured using device tags , which classify and organize endpoints (e.g., by department, OS type, or role). Tag-based grouping allows administrators to apply policies or features (like Live Response) efficiently to specific sets of devices, such as only production servers.

Alternative options such as "Automation level" or "device value" are unrelated - automation level controls auto-remediation, while device value assigns importance for alert prioritization.

Thus, the correct configuration steps are:

* Enable Live Response for Servers under advanced features.
* Apply the configuration to the target device group identified by a device tag .

Final Answer:

* Advanced feature: Live Response for Servers
* For the device group: A device tag

質問**: 140**

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。

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. Azureコネクタ

B. ユーザーエンリッチメント設定

C. 自動ログアップロード設定

D. Microsoft 365 コネクタ

正解: **D** (コメントを発表する)
To investigate threats using data from the unified audit log in Microsoft Defender for Cloud Apps, you mus t first bring that audit log data into the scope of Cloud Apps. The unified audit log is a Microsoft 365 / Purview (formerly Office 365) audit log service, which records user and administrator activities across Microsoft 365 services. Microsoft Defender fo r Cloud Apps can ingest those audit records via a Microsoft 365 / Office 365 connector .
Before logs can flow, you need to ensure that auditing is turned on in Microsoft Purview / Microsoft 365, and then connect Microsoft 365 to Defender for Cloud Apps via the "App connectors # Microsoft 365" option under Cloud Apps settings. Once the Microsoft 365 connector (also known as the Office 365 connector) is configured, Defender for Cloud Apps begins ingesting unified audit log events and making them available for investigation, policy enforcement, anomaly detection, etc.
Here's why the other options are not sufficient:
* The Azure connector is used to bring Azure service logs into Cloud Apps, not Microsoft 365 audit logs.
* User enrichment settings add metadata about users (e.g. departments, manager) to Cloud Apps context but do not by themselves bring audit log events.
* Automatic log upload settings (for example, for firewall or proxy logs) support Cloud Discovery or network log ingestion, not the unified audit log fro m Microsoft 365.
Therefore, to use the unified audit log data for threat investigations in Defender for Cloud Apps, you must first configure the Microsoft 365 connector .

質問: **141**
貴社はMicrosoft Sentinelを使用しています
新任のセキュリティアナリストが、Microsoft Sentinelでインシデントの割り当てと解決ができないと報告している。
アナリストがインシデントの割り当てと解決を行えるようにする必要があります。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。
アナリストにはどのような役割を割り当てるべきですか？
A. Microsoft Sentinel Responder
B. ロジックアプリ貢献者
C. Microsoft Sentinel Reader
D. Microsoft Sentinel 貢献者
正解: **A** (コメントを発表する)
The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege.
Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst ' s needs. Microsoft Sentinel Reader role is not sufficient as it doesn ' t have permission to assign and resolve incidents.
Reference: https://docs.microsoft.com/en-us/azur e/sentinel/role-based-access-control-rbac

質問: **142**
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。
Microsoft Sentinelワークスペースをお持ちです。
Microsoft Sentinelコネクタは、次の表に示すように構成されます。

Connector	Collected log
Microsoft Entra ID	• Audit logs • Microsoft Graph activity logs
Microsoft 365	• Microsoft Exchange Online • Microsoft SharePoint Online • Microsoft Teams

Microsoft Sentinel を使用して、条件付きアクセス ポリシーに関連する疑わしい Microsoft Graph API アクティビティを調査します。以下のアクティビティを検索する必要があります。
* PowerShellを使用して条件付きアクセス ポリシーをダウンロードする
* Microsoft Entra 管理センターを使用して条件付きアクセス ポリシーを更新します。各アクティビティに対してどのテーブルをクエリする必要がありますか? 回答するには、回答領域で適切なオプションを選択します。
注：正解ごとに1ポイントが加算されます。

正解:
Answer Area

Explanation:

For Conditional Access investigations in Microsoft Sentinel, the data source depends on the control plane used. When policies are downloaded via PowerShell , the cmdlets call the Microsoft Graph (e.g., Get- MgIdentityConditionalAccessPol icy). Those Graph req uests are captured by the Microsoft Graph Activity Logs connector and land in the MicrosoftGraphActivityLogs table. This table records the app identity (such as PowerShell/Graph SDK), the API path (like /identity/conditionalAccess/policies), verb (GET), an d result, which is ideal for spotting bulk reads/exports of policy definitions.
When policies are updated in the Microsoft Entra admin center , two streams provide visibility. First, directory auditing writes change events (create/update/delete of Condition al Access policies) to Microsoft Entra Audit logs , surfaced in Sentinel as the AuditLogs table, including the actor, target policy, operation (Update policy), and result. Second, the Entra admin center itself is a first-party application that performs the update by invoking Microsoft Graph ; those API calls are also recorded in MicrosoftGraphActivityLogs (with verb PATCH/POST and the policy resource path).

Therefore, to cover both perspectives- the authoritative audit record and the underlying API activity - you should query AuditLogs and MicrosoftGraphActivityLogs for updates, and MicrosoftGraphActivityLogs for downloads executed through PowerShell.

質問: **143**
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションを所有しており、そのサブスクリプションには100台のLinux仮想マシンが含まれています。
Microsoft Sentinelを使用して仮想マシンを監視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。
管理業務の手間を最小限に抑える
ログデータの読み取りに必要な解析処理を最小限に抑える
何を設定すればよいですか？
A. REST API統合
B. SysJogコネクタ
C. ログ分析データコレクターAPI
D. 共通イベントフォーマット (CEF) コネクタ
正解: **D (**コメントを発表する**)**
To ingest security logs from Linux virtual machines into Microsoft Sentinel efficiently, Microsoft recommends using the Common Event Format (CEF) connector .
The CEF connector allows Linux machines to send logs in a structured, normalized format via Syslog , minimizing custom parsing in Sentinel. The CEF schema is widely adopted by SIEM and security products, ensuring compatibility and simplified analytics rule creation.
How it works:
* The Linux VMs send logs to a local Syslog daemon.
* The Syslog daemon forwards the logs (in CEF format) to the Log Analytics workspace connected to Microsoft Sentinel.
* Sentinel automatically maps CEF fields, minimizing parsing and normalization effort.
Why not the others:
* REST API integration: Requires custom scripting and parsing - high admin effort.
* Syslog connector: Sends raw logs that need additional parsing and normalization.
* Log Analytics Data Collector API: Used for custom ingestion scenarios, not scalable for 100 VMs.
# Correct answer: D. a Common Event Format (CEF) connector

質問: **144**
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. デバイスを隔離する
C. メールメッセージをソフト削除する
D. メールメッセージを強制削除します
正解: **(**正解を表示します**)**

質問: **145**
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: (正解を表示します)

Roles in Microsoft Sentinel are designed for least privilege. The Azure Sentinel Responder role allows analysts to view, assign, update, and dismiss incidents, change status/severity, and add comments-exactly the actions a Tier-1/Tier-2 analyst needs for day-to-day triage. Azure Sentinel Reader is view-only and cannot change incident state. Azure Sentinel Contributor is broader than needed (it includes creating/editing analytics rules and other configuration). Logic App Contributor pertains to playbook authoring, not incident handling.
Therefore, to let a new analyst assign and dismiss incidents while honoring least privilege, assign Azure Sentinel Responder.

質問: **146**

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。
AD DSオブジェクトを列挙するには、AD DSユーザーによるLDAPリクエスト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:

Explanation:
1. IdentityQueryEvents When considering a table with AccountSid and it ' s about the LDAP request, it is " IdentityQueryEvents. "
2. isnotempty For determining whether there is a value in the AccountSid, it is " isnotempty. "

質問: **147**

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ポイント獲得できます。

Values

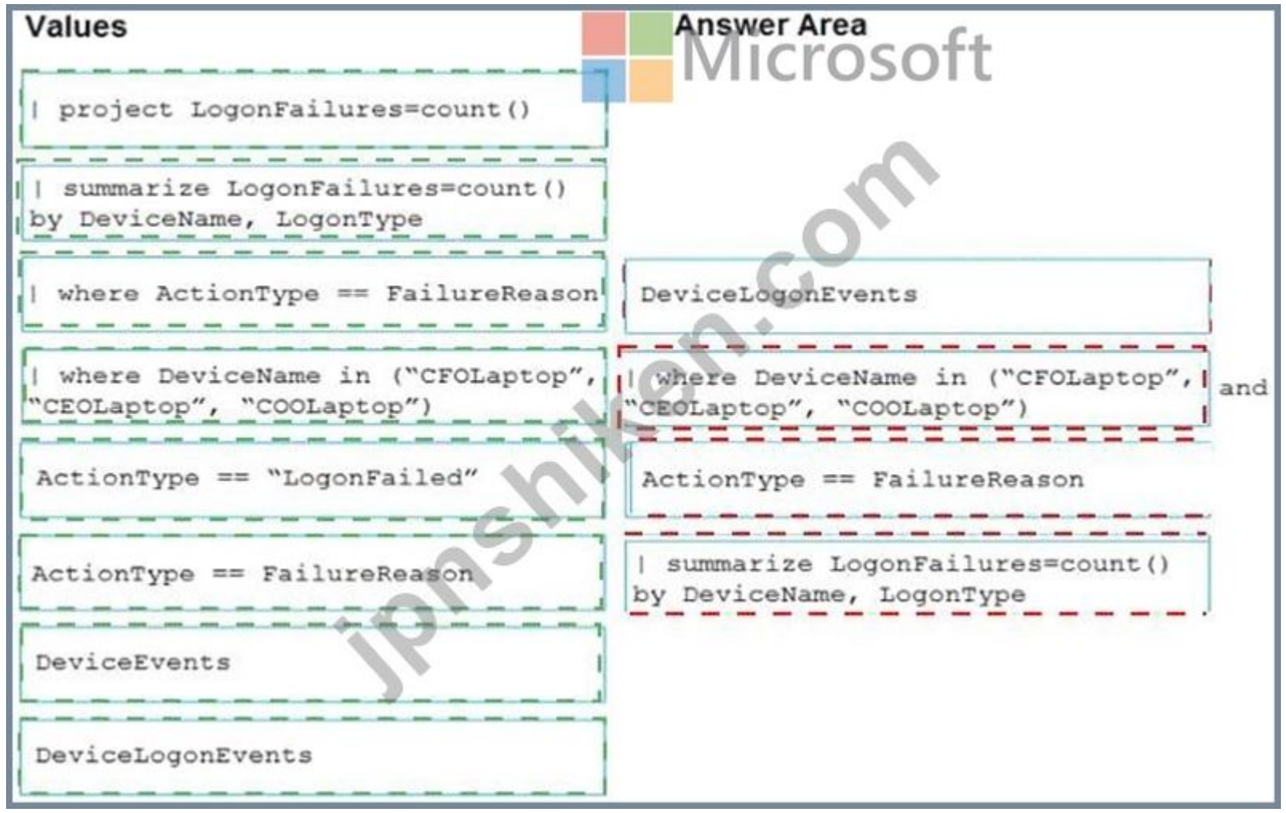
- `| project LogonFailures=count()`
- `| summarize LogonFailures=count() by DeviceName, LogonType`
- `| where ActionType == FailureReason`
- `| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")`
- `ActionType == "LogonFailed"`
- `ActionType == FailureReason`
- `DeviceEvents`
- `DeviceLogonEvents`

Answer Area

`| where ActionType == FailureReason` [ ]

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

正解:



Explanation:

In Microsoft 365 Defender advanced hunting , interactive sign-in activity on endpoints is recorded in the DeviceLogonEvents table. This table includes fields such as DeviceName , ActionType , and LogonType .

For failed authentications, the normalized ActionType value is " LogonFailed " . To count failures per device (and optionally by logon type), you filter the target devices and failed-action events, then summarize.

The query pattern is:

* Start from DeviceLogonEvents (the canonical table for endpoint logon successes/failures).
* Apply a where clause to limit to the three devices using DeviceName in (...) .
* Add an and condition for ActionType == " LogonFailed " to select only failed authentications.
* Use summarize with count() to total failures, grouping by DeviceName and LogonType to see counts per device and logon type.

Assembled query:

DeviceLogonEvents

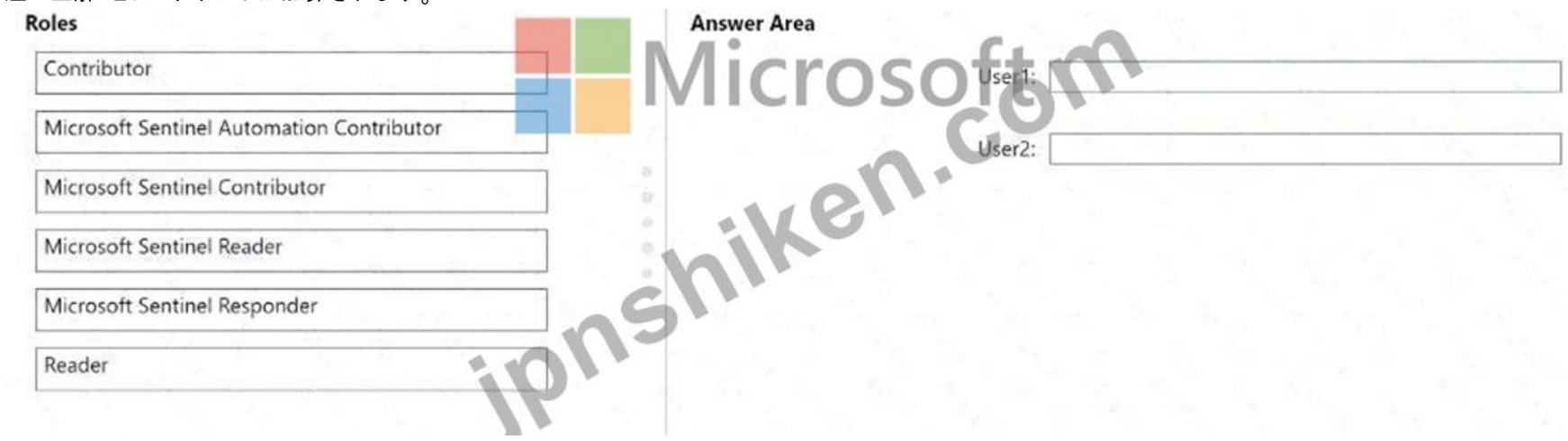
| where DeviceName in (" CFOLaptop " , " CEOLaptop " , " COOLaptop ") and ActionType == " LogonFailed "
| summarize LogonFailures=count() by DeviceName, LogonType
This precisely returns the count of failed sign-in authentications on the specified three devices.

質問**: 148**
セキュリティ管理者は、ストレージ アカウントにアップロードされた潜在的なマルウェアやブルート フォース攻撃の成功などのアクティビティに関する電子メール アラートを Azure Defender から受け取ります。
セキュリティ管理者は、マルウェア対策アクションの失敗や不審なネットワーク アクティビティなどのアクティビティに関する電子メール アラートを受信しません。アラートは Azure Security Center に表示されます。
セキュリティ管理者がすべてのアクティビティに関する電子メール アラートを受信するようにする必要があります。
セキュリティ センターの設定で何を構成する必要がありますか?
A. 電子メール通知の重大度レベル
B. クラウド コネクタ
C. Azure Defender プラン
D. 脅威検出の統合設定
正解**: (**正解を表示します**)**
Reference:
In Azure Security Center (now known as Microsoft Defender for Cloud), email notifications for security alerts are controlled by the Email notifications settings under Environment settings # Email notifications .
These settings allow administrators to specify who receives notifications and what severity levels (High, Medium, Low) will trigger email alerts.
By default, Security Center sends email notifications only for High severity alerts. This explains why the administrator receives alerts for "potential malware uploaded" or "brute-force attacks" (both high severity) but not for "antimalware action failed" or "suspicious network activity" (which are usually medium or low severity).
To ensure all alert types trigger an email, you must change the severity level of email notifications to include Medium and Low .
Microsoft documentation states:
"Security Center can send email notifications about new security alerts. You can define the recipients and choose to receive notifications for High, Medium, and Low severity alerts. By default, only High severity alerts trigger notifications." The other options are incorrect:
(B) Cloud connector - used for connecting AWS or GCP environments, unrelated to email alert settings.
(C) Azure Defender plans - control which resources are protected, not notification delivery.
(D) Integration settings for Threat detection - manage data sources and integrations, not email alerts.
Therefore, the correct answer is A. the severity level of email notifications .

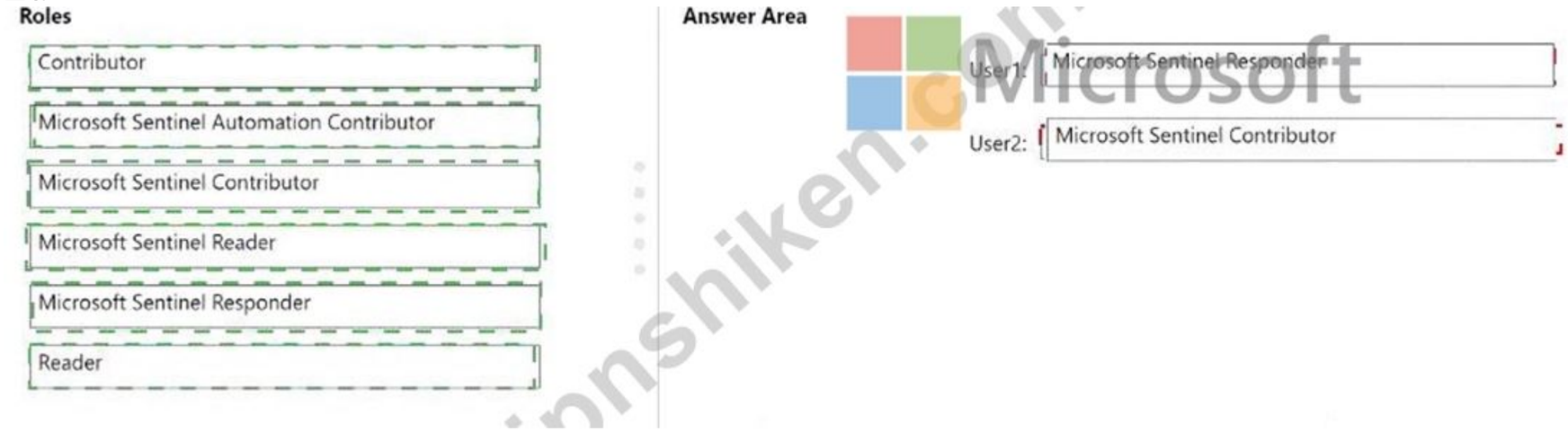
質問**: 149**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Azure Sentinel を構成しています。
悪意のある IP アドレスからの Azure 仮想マシンへのサインインが検出された場合は、Azure Sentinel でインシデ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)
A scheduled query rule in Azure Sentinel is the correct method to detect and generate alerts/incidents based on specific data patterns such as sign-ins from malicious IPs. The scheduled rule can run periodically (e.g., every 5 minutes or hour), execute a KQL query filtering for malicious IPs, and create incidents automatically when matches are found. This satisfies the goal of automatically creating incidents for suspicious sign-ins.

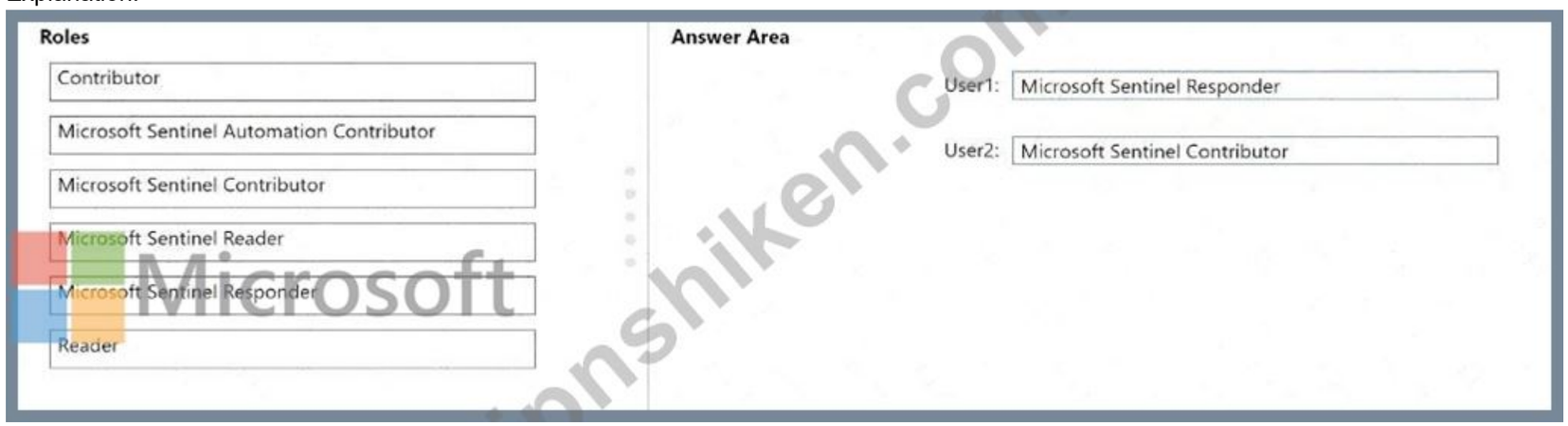
質問: **150**
User1とUser2という2人のユーザーと、workspace1というMicrosoft Sentinelワークスペースを含むAzureサブスクリプションがあります。ユーザーがworkspace1で以下のタスクを実行できるようにする必要があります。
* ユーザー1は、インシデントを却下したり、インシデントをユーザーに割り当てることができる必要があります。
* ユーザー2は分析ルールを変更できる必要があります。
解決策は、最小権限の原則に基づかなければならない。
各ユーザーにどの役割を割り当てるべきでしょうか？回答するには、適切な役割を正しいユーザーにドラッグしてください。各役割は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



In Microsoft Sentinel , different built-in roles provide access at varying levels of capability, following the principle of least privilege .

* Microsoft Sentinel Responder
* Purpose: Designed for SOC analysts responsible for h andling and responding to incidents.
* Capabilities:
* View and investigate incidents.
* Assign incidents , dismiss incidents , and change incident statuses .
* Respond to alerts but cannot modify Sentinel configuration or analytics rules .
* # This matches the requirem ents for User1 , who needs to dismiss and assign incidents .
* Microsoft Sentinel Contributor
* Purpose: Intended for security engineers or Sentinel administrators .
* Capabilities:
* Create, edit, and delete analytics rules , workbooks , hunting queries , and automation rules .
* Manage data connectors and configuration.
* Cannot assign permissions but can change Sentinel resources.
* # This matches the requirements for User2 , who must be able to modify analytics rules .

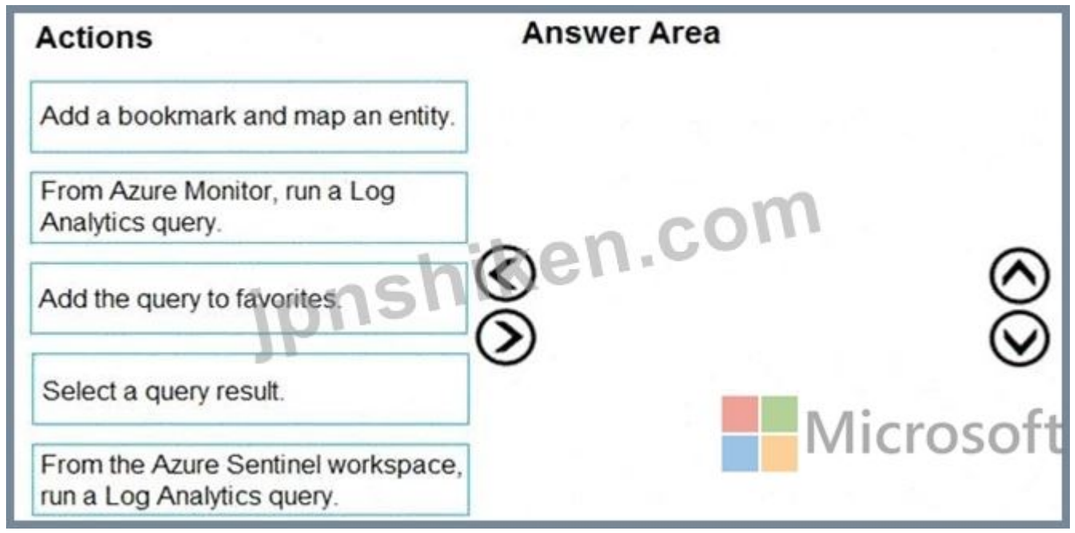
Other roles for reference:

* Microsoft Sentinel Re ader: View-only permissions.
* Microsoft Sentinel Automation Contributor: Allows playbook and automation editing.
* Contributor/Reader: General Azure roles, not Sentinel-specific.

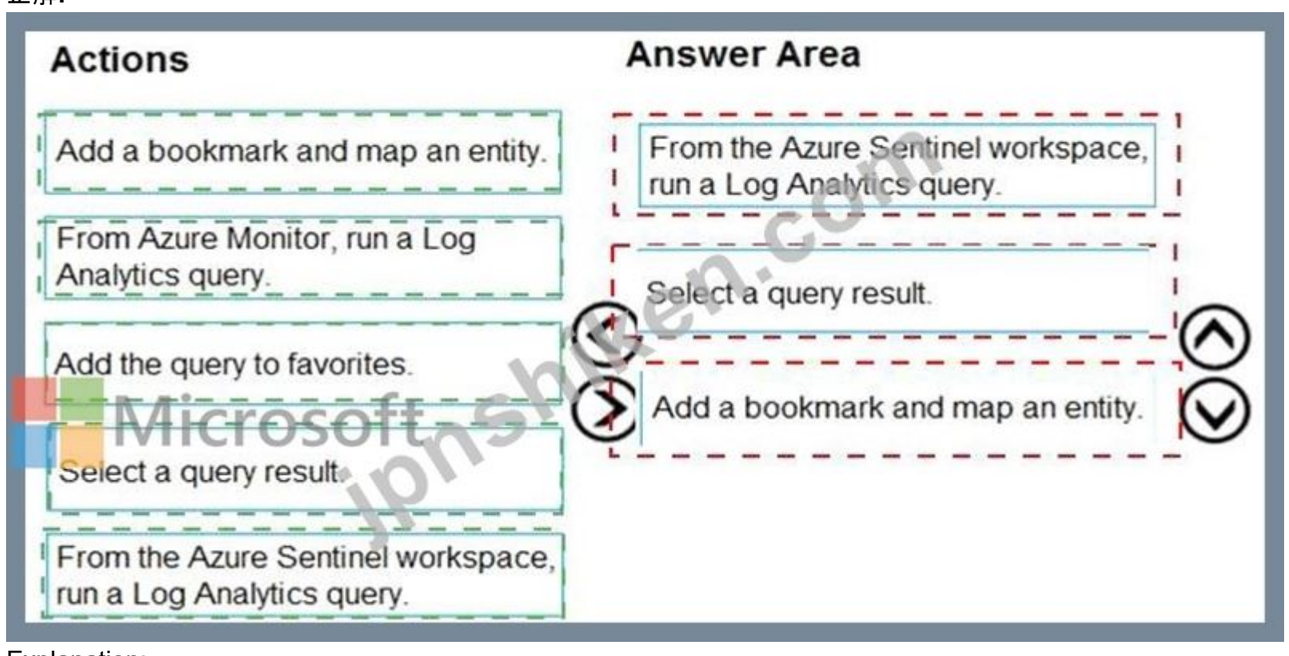
質問**: 151**

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。

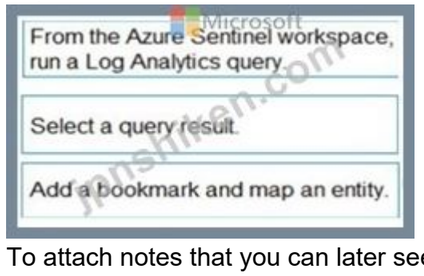
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



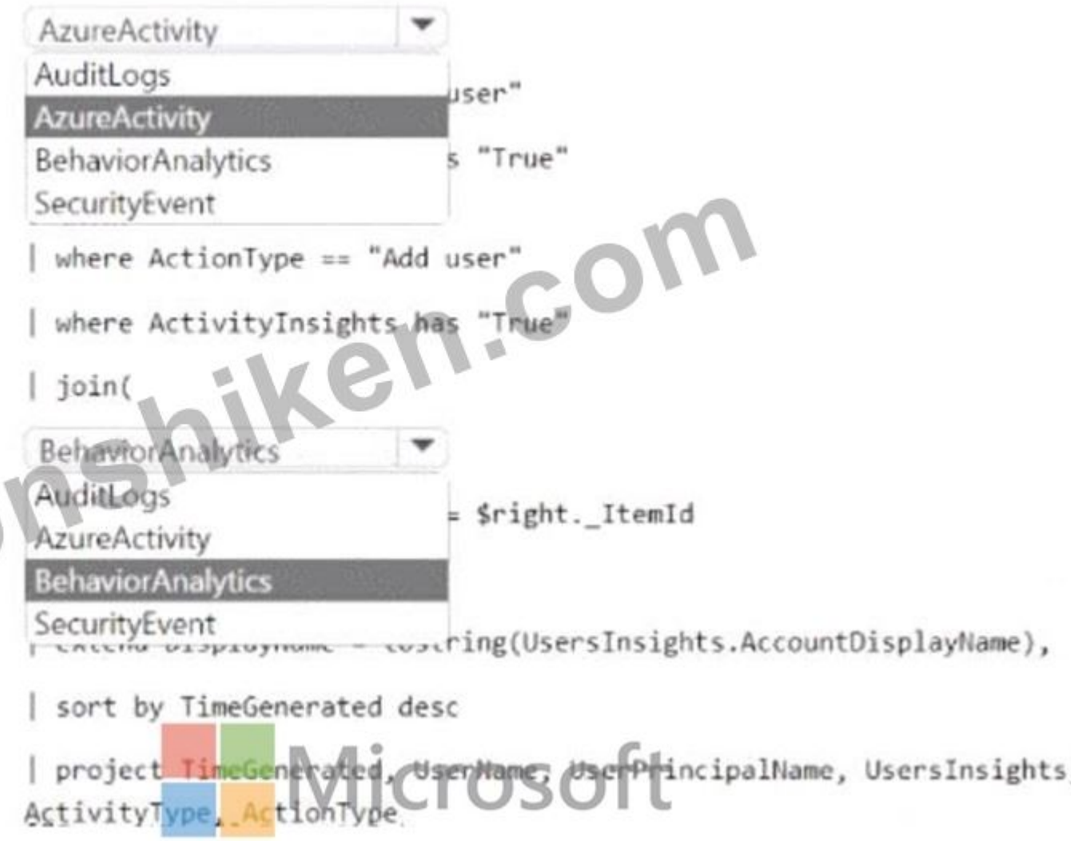
To attach notes that you can later see during investigations and hunting, you use Bookmarks in Microsoft Sentinel. Bookmarks are created from the Hunting (or Logs) experience inside the Sentinel workspace and let you pin a specific query result (including IPs, accounts, hosts) with notes, tags, and mappe d entities so it appears in the investigation graph and is easily referenceable. The correct workflow is: first, run your KQL query from the Microsoft Sentinel workspace (not from generic Azure Monitor), because Sentinel's hunting experience is where bookmarks integrate with incidents and the

investigation graph. Next, select a specific query result that represents the suspicious activity (e.g., a data access event from the target IP). Finally, create a Bookmark and map the relevant entity (IP address, Account, etc.) while adding your notes . Mapping the entity ensures the bookmarked event is connected in the investigation graph; the notes provide the narrative /context you need when pivoting later. Adding the query to favorites is optional for convenience but does not attach notes to a specific event, and running the query from Azure Monitor would not place the bookmark within Sentinel's investigation context.

質問: **152**
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. オートメーションランブックオペレーター
C. Azure Sentinel 貢献者
D. ロジックアプリ貢献者
正解: **(正解を表示します)**
Azure Sentinel "playbooks" are Azure Logic Apps . Granting the minimal permissions to configure (create /edit) playbooks requires the Logic App Contributor role on the resource group where the playbooks reside.
This satisfies the business requirement to use least privilege and specifically enables admin1 to design, modify, and manage Logic Apps that Sentinel automation rules or analytics rules will invoke. Roles like Automation Operator or Automation Runbook Operator apply to Azure Automation , not Logic Apps, and therefore don't allow creating or editing Sentinel playbooks. Azure Sentinel Contributor allows managing Sentinel resources (incidents, analytics rules, workbooks) but, by itself, does not grant permissions to author Logic Apps. Assigning Logic App Contributor provides precisely what is needed to configure Sentinel playbooks without unnecessary broader permissions.

質問: **153**
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



正解:

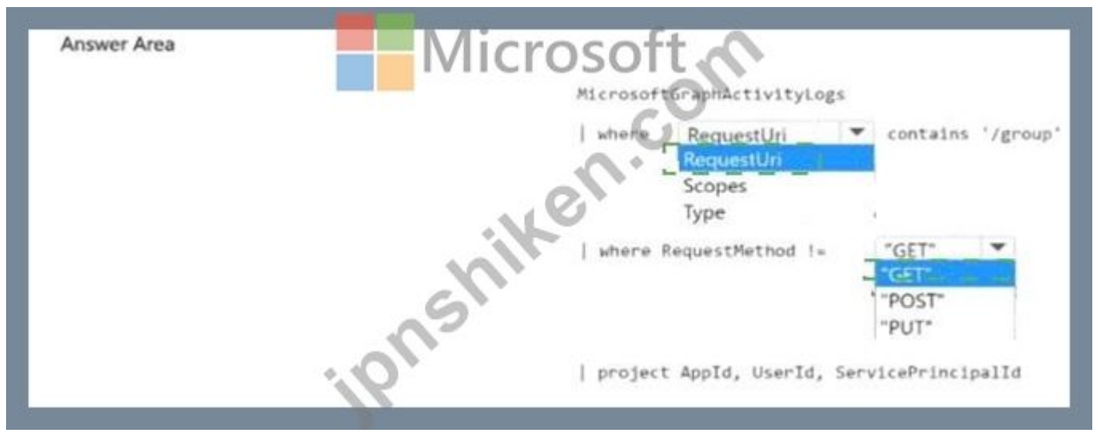
Answer Area

Explanation:
First table: BehaviorAnalytics
Joined table: AuditLogs
To detect when a user creates an unusually large number of Azure AD user accounts in Microsoft Sentine l, you should leverage UEBA signals from the BehaviorAnalytics table and enrich them with Azure AD audit data from AuditLogs . The BehaviorAnalytics table contains UEBA-derived insights (for example, the ActivityInsights flag and UsersInsights) and normaliz ed activity fields such as ActionType (e.g., " Add user
"). Filtering BehaviorAnalytics for ActionType == " Add user " and ActivityInsights has " True " targets activities that the UEBA engine already assessed as anomalous, reducing noise and focusing on outlier s.
Then, join these anomalies to the AuditLogs table to pull authoritative Azure AD audit details (target object, initiator, correlation, and operation context). This combination aligns with Sentinel guidance: use BehaviorAnalytics for anomaly detection an d AuditLogs for the Azure AD operational record. Sorting by TimeGenerated and projecting user and insight fields completes the hunting query so analysts can review who triggered unusual "Add user" bursts and with what context.
Therefore, complete the query by selecting BehaviorAnalytics as the primary dataset and AuditLogs in the join(...) .

質問**: 154**
あなたはMicrosoft 365のサブスクリプションをお持ちです。
グループの変更または削除を要求したすべてのセキュリティプリンシパルを特定する必要があります。KQLクエリはどのように作成すればよいでしょうか？回答するには、回答領域で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

正解:



Explanation:

To find all security principals (users or service principals/apps) that changed or deleted groups , you should query MicrosoftGraphActivityLogs and filter for requests targeting the groups endpoint, then exclude read-only operations. The RequestUri field contains the full Graph URL that the principal called (e.
g., /v1.0/groups/{id}), so filtering where RequestUri contains " /group " (or " /groups ") isolates group- related operations. Changes and deletions are non-read HTTP verbs such as POST , PATCH , PUT , and DELETE . The simplest way to capture all of them is to exclude reads: where RequestMethod != " GET " .
Finally, projecting AppId , UserId , and ServicePrincipalId returns the identities (user or app) behind each request, which are the "security principals" you need to report.
So the completed KQL is:
MicrosoftGraphActivityLogs
| where RequestUri contains " /group "
| where RequestMethod != " GET "
| project AppId, UserId, ServicePrincipalId

質問: **155**

Microsoft Defender for DevOps を使用する Azure DevOps 組織があります。この組織には、Repo1 という名前の Azure DevOps リポジトリと、Pipeline1 という名前の Azure Pipelines パイプラインが含まれています。

Pipeline1は、Repo1に保存されているコードをビルドおよびデプロイするために使用されます。

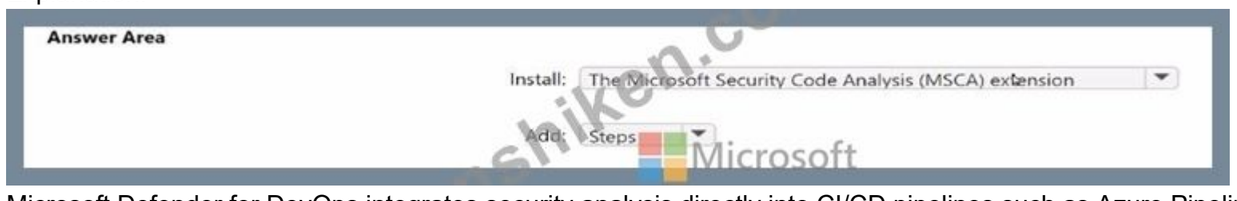
Pipeline1の実行時に、Microsoft Defender for CloudがRepo1内のコードのシークレットスキャンを実行できるようにする必要があります。

組織に何をインストールし、パイプライン ｢?｣のYAMLファイルに何を追加すべきでしょうか？回答するには、回答エリアで適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

正解:

Explanation:



Microsoft Defender for DevOps integrates security analysis directly into CI/CD pipelines such as Azure Pipelines , GitHub Actions , and others. To enable secret scanning (and other code security checks) during the execution of a pipeline in Azure DevOps , the correct integration is through the Microsoft Security DevOps (MSDO) extension - not the older Microsoft Security Code Analysis (MSCA) extension.

Step 1: Install the Microsoft Security DevOps extension Microsoft documentation (Defender for Cloud # Defender for DevOps integration guide) clearly states that:

"To enable scanning and policy enforcement for Azure DevOps pipelines, install the Microsoft Security DevOps extension from the Azure DevOps Marketplace. This extension integrates with Microsoft Defender for Cloud to perform security scans, including secret detection, infrastructure-as-code analysis, and dependency vulnerability checks." The older Microsoft Security Code Analysis (MSCA) extension has been superseded by Microsoft Security DevOps , which provides broader coverage and native Defender for Cloud integration.

Step 2: Add the MSDO scanner steps to the YAML pipeline After installing the extension, you must modify the pipeline definition (YAML) to add MSDO scanning steps .

The syntax typically looks like this:

steps:

- task: MicrosoftSecurityDevOps@1

displayName: ' Run Microsoft Security DevOps '

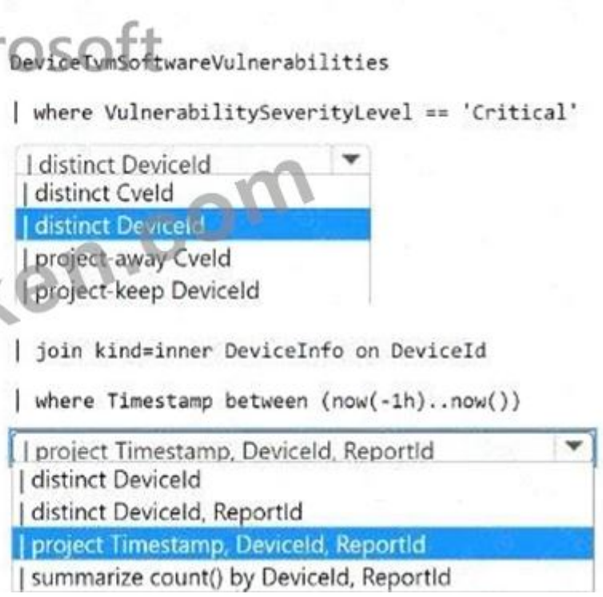
This step runs all configured scans (including secret scanning) automatically each time the pipeline runs. You add it under the steps section because it represents a specific task in the pipeline workflow.
Final Answers:
* Install: The Microsoft Security DevOps extension
* Add: Steps

質問**: 156**
Azure サブスクリプションには、app1 という名前の Azure ロジック アプリと、Azure AD コネクタを持つ Microsoft Sentinel ワークスペースが含まれています。Microsoft Sentinel が Azure AD で生成されたアラートを検出したときに app1 が起動するようにする必要があります。最初に何を作成する必要がありますか？
A. リポジトリ接続
B. ウォッチリスト
C. 分析ルール
D. 自動化ルール
正解**: (**正解を表示します**)**
The goal is to automatically execute the Azure Logic App (app1), which is known as a Playbook in Microsoft Sentinel, in response to a newly created alert.
* The Playbook (Logic App): An Azure Logic App used for security response in Microsoft Sentinel is called a Playbook. It is a workflow that must start with a trigger, typically the Microsoft Sentinel incident or Microsoft Sentinel alert trigger.
* The Trigger Mechanism (Automation Rule): To run a playbook automatically when an alert or incident is created, you must use a Microsoft Sentinel Automation Rule .
* Required Flow: The Logic App (app1) acts as the action to be performed, but it must be called by an automation component. The recommended and modern approach for linking automated actions (playbooks) to alerts and incidents in Microsoft Sentinel is via Automation Rules .
The sequence of operations is:
* The Azure AD Connector ingests data into the Microsoft Sentinel workspace.
* A corresponding Analytics Rule (Option C) detects a threat in that data and generates an Alert . This alert usually leads to the creation of an Incident .
* The Automation Rule (Option D) is configured to:
* Trigger: When an incident is created (or when an alert is created).
* Condition: Filter for the specific alert or incident (e.g., where the Analytic Rule Name is the one that detects the Azure AD threat).
* Action: Select the Run playbook action and specify app1 .
While an Analytics Rule (C) generates the initial alert, the Automation Rule (D) is the specific component that takes that alert/incident as input and performs the action of launching the Logic App (playbook) automatically. The ability to invoke playbooks directly from Analytics Rules (the " Alert automation (classic)
" method) is deprecated in favor of using Automation Rules, making the Automation Rule the correct and contemporary first step for this requirement.

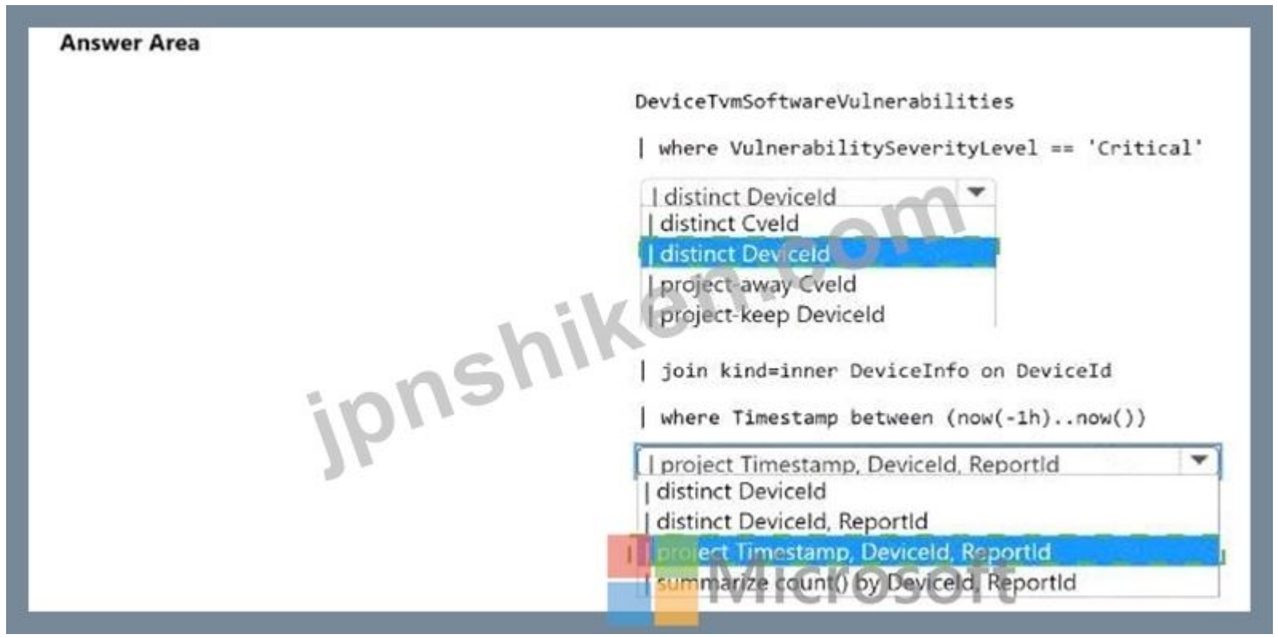
質問**: 157**
Azure Defender を使用しています。
機密情報を含む Azure ストレージ アカウントをお持ちです。
誰かが不審な IP アドレスからストレージ アカウントにアクセスした場合は、PowerShell スクリプトを実行する必要があります。
どの 2 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure Security Center から、ワークフローの自動化を有効にします。
B. 手動トリガーを持つ Azure ロジック アプリを作成します
C. 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**)**
To run a PowerShell script when a suspicious-IP access alert is raised for Storage, use Workflow automation in Defender for Cloud to trigger a Logic App whenever a matching security alert occurs. The Logic App should use the Azure Security Center (Defender for Cloud) alert trigger , and from there you can call an Automation Runbook (PowerShell) or another action to execute your script. A manual or HTTP trigger isn't needed because the flow must start automatically from the security alert, and an AAD app registration is not required for the basic alert-triggered flow.

質問: **158**
Microsoft Defender for Endpoint を使用する Microsoft 365 E5 サブスクリプションをお持ちの場合、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



正解:

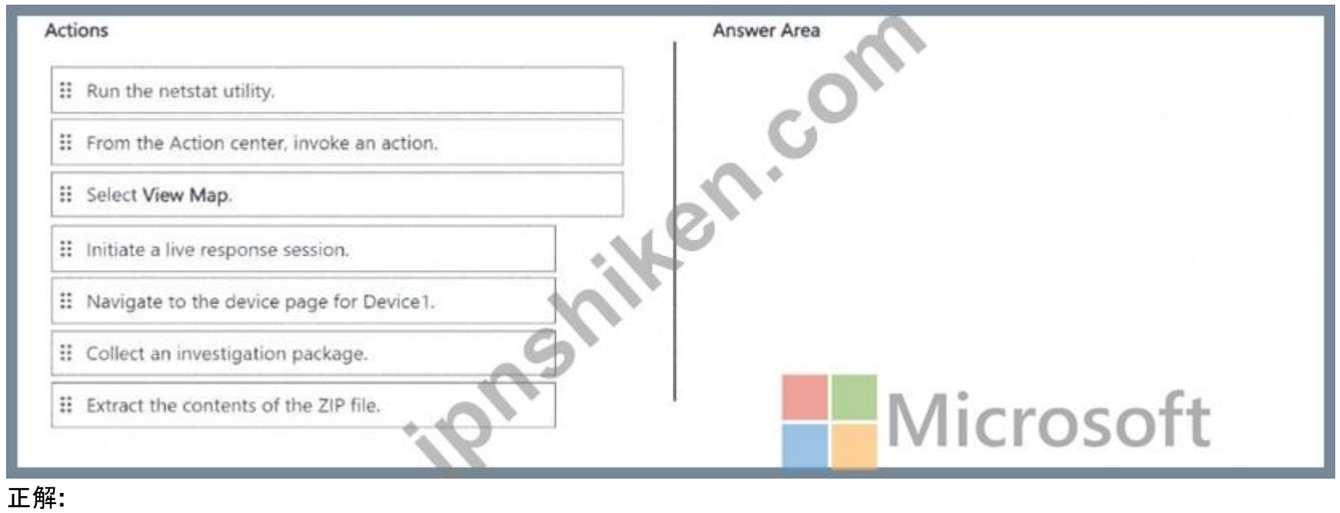


質問: **159**

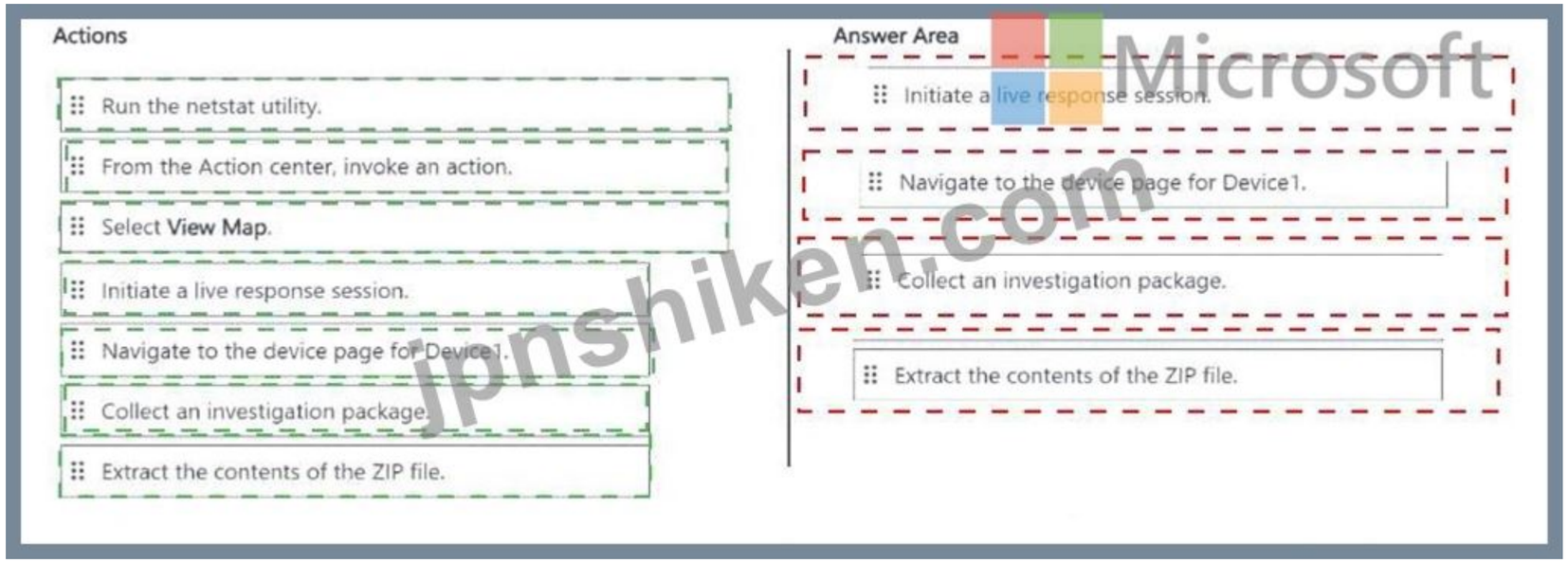
オンプレミスの Windows 11 Pro デバイス (Device1 という名前) があり、Microsoft Defender for Endpoint にオンボーディングされています。Microsoft 365 サブスクリプションをお持ちです。

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。

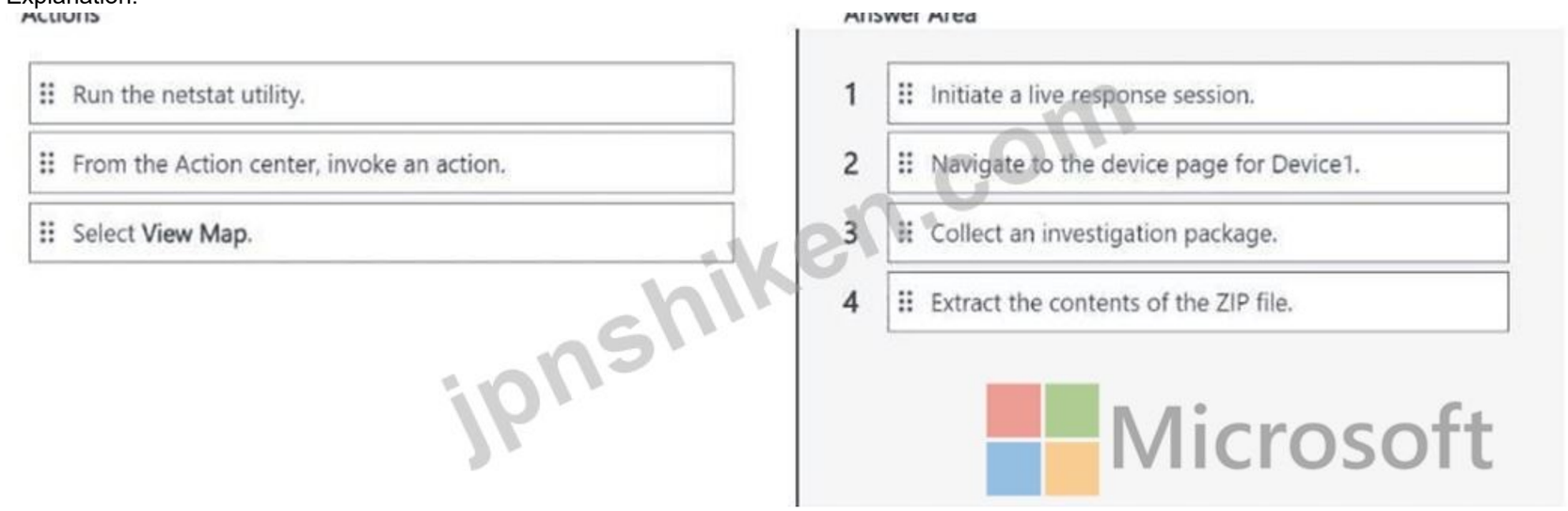
Microsoft Defender ポータルで、どの 4 つの操作を順番に実行する必要がありますか？回答するには、操作の一覧から適切な操作を回答欄に移動し、正しい順序に並べ替えてください。



正解:



Explanation:



In Microsoft Defender for Endpoint, the quickest way to enumerate running processes and their open network connections on a Windows device is to use the built-in Investigation package feature from the device page.

Collecting an investigation package executes a set of diagnostics on the endpoint and bundles artifacts- including process lists , network connections (netstat ou tput) , services, autoruns, scheduled tasks, and other forensic logs- into a ZIP file. After you trigger Collect investigation package on the device page , the job appears in the Action center ; once completed, you open that action and download the package. Finally, extract the ZIP to review the CSV/TXT outputs that show active processes and network connectivity, satisfying the requirement with minimal administrative effort and without initiating a live response session or running interactive commands manually.

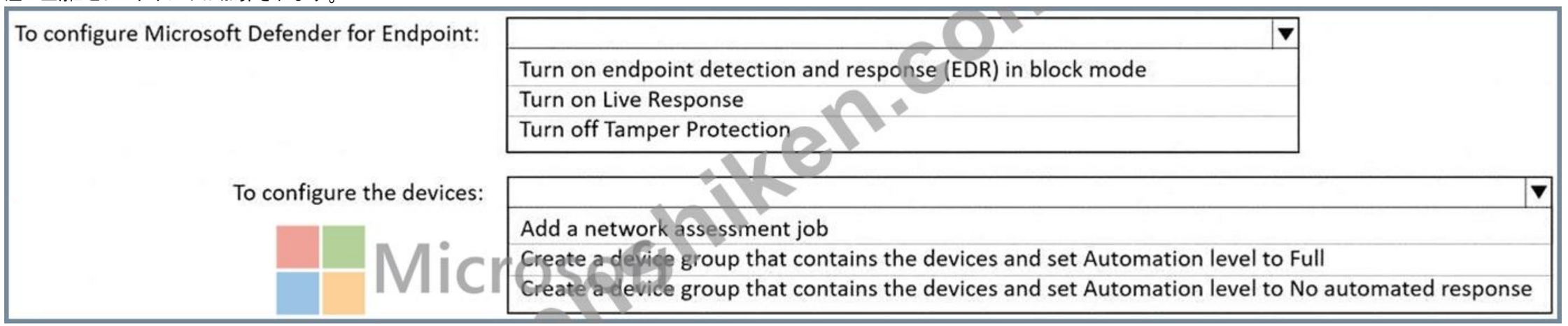
質問: **160**

Azure Sentinel を使用しています。

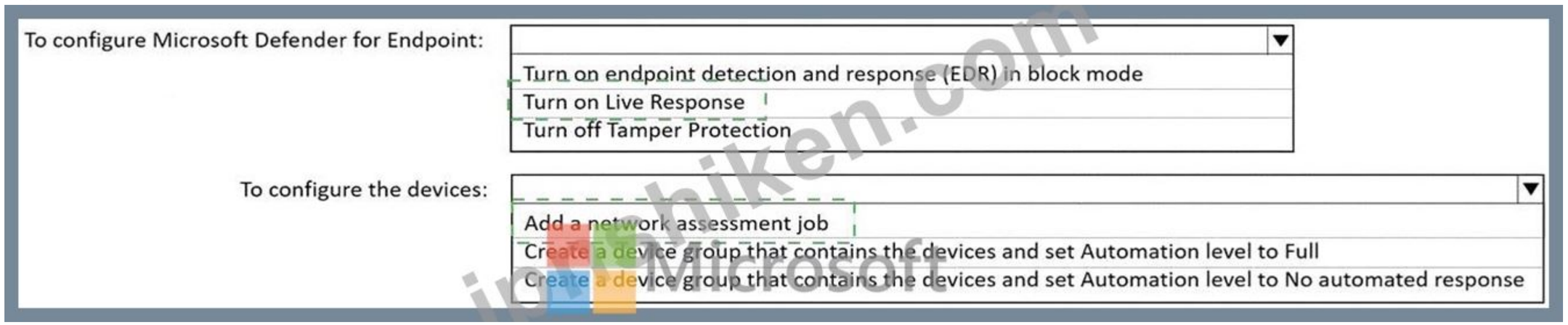
組み込みロールを使用して、セキュリティ アナリストにカスタム Azure Sentinel ブックのクエリを編集する機能を提供する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。

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: **(**正解を表示します**)**
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: **161**
お客様は、Microsoft Defender for Endpointに登録された200台のWindows 10デバイスを含むMicrosoft 365 E5サブスクリプションをご利用中です。
ユーザーがMicrosoft 365 Defenderポータルから直接リモートシェル接続を使用してデバイスにアクセスできることを確認する必要があります。このソリューションは、最小権限の原則に従う必要があります。
Microsoft 365 Defender ポータルで何をすべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
htt ps://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?
view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365- worldwide

質問**: 162**
Azure Information Protectionの要件を満たす必要があります。最初に何を構成すればよいでしょうか？
A. Microsoft Defender セキュリティ センターのデバイスの状態とコンプライアンス レポートの設定
B. AzureポータルからのAzure Information Protectionのスキャナクラスタ
C. AzureポータルからのAzure Information Protectionのコンテンツスキャンジョブ
D. Microsoft Defender セキュリティ センターの設定から高度な機能
正解**: (**正解を表示します**)**
To show labeled files from Windows 10 endpoints in the Azure Information Protection - Data discovery dashboard , you must first enable the built-in integration between Microsoft Defender for Endpoint and Azure Information Protection (AIP) . This is turned on in the Microsoft Defender Securit y Center under Settings # Advanced features . When enabled, Defender for Endpoint inventories sensitivity labels seen on files across managed Windows devices and streams that telemetry to the AIP Data discovery experience, providing visibility into where la beled data resides on endpoints. Scanner clusters and content scan jobs in AIP are intended for on-premises repositories (file shares/SharePoint servers), not for endpoint discovery.
Device health/compliance reports do not surface or forward label inventor y to AIP. Therefore, the first configuration step is enabling the AIP integration advanced feature in Defender for Endpoint so labeled files on Windows clients appear in the AIP Data discovery dashboard.
Topic 3, Adatum Corporation
Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.
The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.
com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group! that syncs with adatum.com.
All the users at Adatum are assigned a Microsoft 365 E5 license and an Azure Active Directory Perineum 92 license.
The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.
com tenant, and the resources shown in the following table.

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

The on-premises network contains the resources shown in the following table.

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

Adatum plans to perform the following changes;

* Implement a query named rulequery1 that will include the following KQL query.

```
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
```

* Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.

Adatum identifies the following Microsoft Defender for Cloud requirements:

* The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
* Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
* Server2 must be excluded from agentless scanning.

Adatum identifies the following Microsoft Sentinel requirements:

* Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
* Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
* Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
* Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company ' s SecOps team.
* Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
* Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account
* Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
* Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
* Minimize the overhead associated with queries that use ASIM parsers.
* Ensure that the Group1 members can create and edit playbooks.
* Use built-in ASIM parsers whenever possible.

Adatum identifies the following business requirements:

* Follow the principle of least privilege whenever possible.
* Minimize administrative effort whenever possible.

Directory Perineum 92 license.

質問: **163**
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. エンティティマッピング
C. クエリルール
D. アラート自動化設定
正解: **D (**コメントを発表する**)**
When you create a Near-Real-Time (NRT) analytics rule in Microsoft Sentinel , the rule runs every minute and triggers almost immediately when matching events are ingested. These NRT rules are designed for time- sensitive detections, such as when you need to respond quickly to activity from connectors like Azure Activity .
However, NRT rules do not generate incidents directly . Instead, they produce alerts , which can then trigger playbooks or automations via the Alert automation settings section.
* A. Incident automation settings: This applies to standard scheduled analytics rules that create incidents , not NRT rules. Since NRT rules generate alerts (not incidents), this option would not apply.
* B. Entity mapping: This is used to map data fields (like Account, Host, IP) for better investigation, but it does not control playbook execution.
* C. The query rule: The query defines what data triggers the rule, not the automation or playbook execution. The playbook is attached separately.
* D. Alert automation settings: # According to Microsoft documentation, "To automatically run a playbook when an alert is created by a near-real-time rule, configure the playbook in the Alert automation settings section." This allows the playbook to run immediately when the alert is generated, achieving near-real-time response with minimal latency.
Detailed reasoning:

質問: **164**
Microsoft Sentinelワークスペースには、以下のAdvanced Security Information Model(ASIM)パーサーが含まれています。
* _Im_ProcessCreate
* InProcessCreate
vimProcessCreate という名前の、ソース固有の新しいパーサーを作成します。
以下の要件を満たすようにパーサーを修正する必要があります。
* すべての ProcessCreate パーサーを呼び出します。
* フィールドをプロセススキーマに標準化する。
各要件を満たすために、どのパーサーを変更する必要がありますか？回答するには、適切なパーサーを正しい要件にドラッグしてください。各パーサーは、1回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注：正解ごとに1ポイントが加算されます。

正解:

Explanation:

Microsoft Sentinel uses the Advanced Security Information Model (ASIM) to normalize logs into a consistent schema, enabling unified queries, analytics rules, and hunting queries across multiple data sources.

Each ASIM function has a structured parser hierarchy , typically consisting of:

* A master (or orchestrator) parser , which aggregates and calls all source-specific parsers.
* Source-specific parsers , which map raw data from each data source (like Windows SecurityEvents, Sysmon, or custom logs) to the ASIM schema fields.

In the case of ProcessCreate events:

* _Im_ProcessCreate is the master parser . Its role is to call all ProcessCreate parsers , including both built-in and custom ones (for example, imProcessCreate , vimProcessCreate , or other vendor-specific parsers).
* Parsers like imProcessCreate (for native sources) and vimProcessCr eate (for custom or vendor-specific sources) are source-specific parsers . They are responsible for standardizing and mapping raw fields into the ASIM Process schema , ensuring consistent naming such as ActorProcessName , TargetProcessName , and TargetProcessC ommandLine .

Based on Microsoft's ASIM documentation: "The _Im_ functions are orchestrators that call all source- specific parsers. Each im or vim parser converts native data into the ASIM schema for its respective source." Therefore:

* To call all ProcessCrea te parsers , modify _Im_ProcessCreate .
* To standardize fields to the Process schema , modify vimProcessCreate (the new source-specific parser you created).

Final Answers:

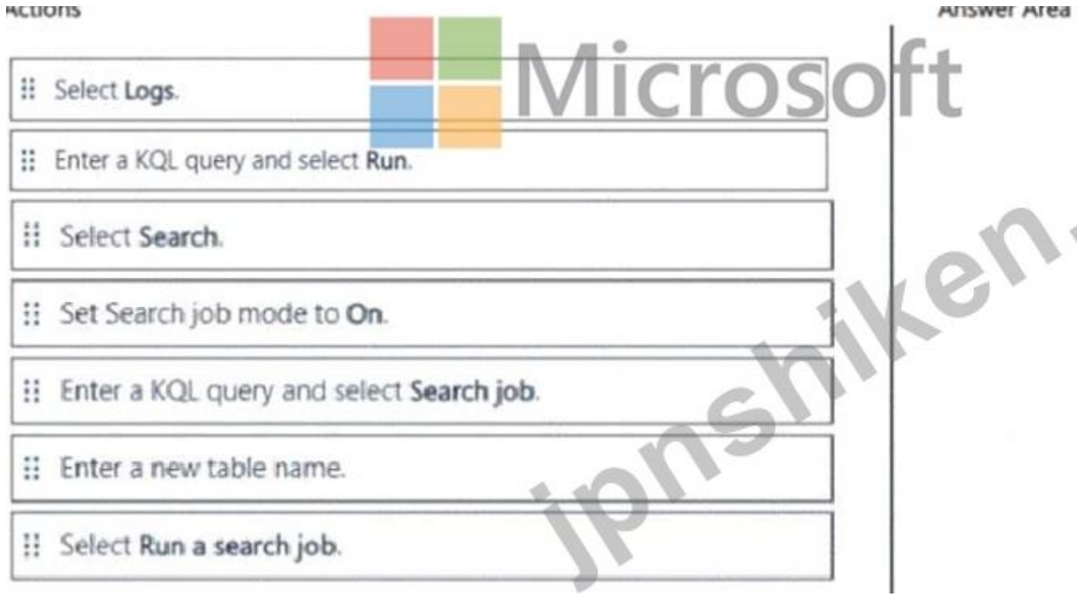
* Call all the ProcessCreate parsers: _Im_ProcessCreate
* Standardize fields to the Proces s schema: vimProcessCreate

質問**: 165**

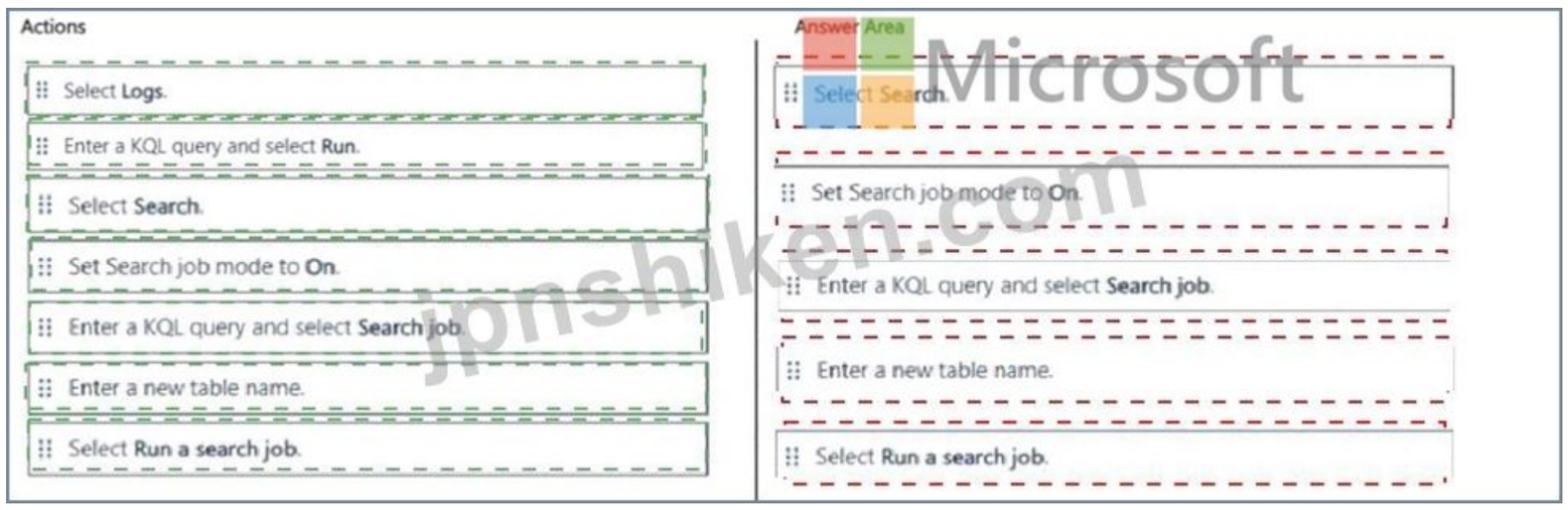
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。

KQLクエリを検索ジョブとして実行する必要があります。

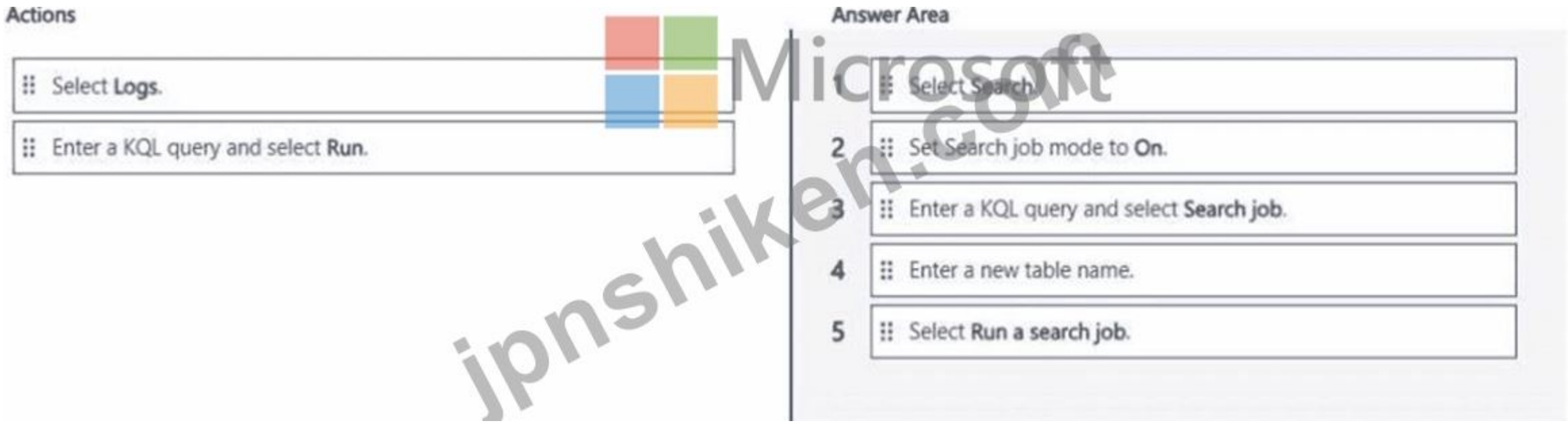
ワークスペース1で実行すべき5つの操作はどれですか？回答するには、操作リストから適切な操作を回答欄に移動し、正しい順序に並べ替えてください。



正解:



Explanation:



質問: **166**

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。

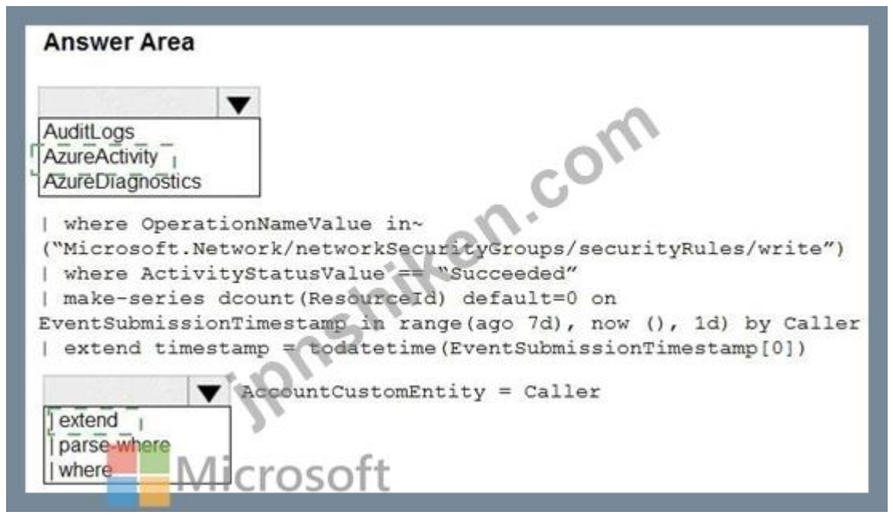
* 同一のセキュリティプリンシパルによって行われたネットワークセキュリティグループ(NSG)のルールに対する異常な数の変更を特定します。

* セキュリティ プリンシパルを Microsoft Sentinel エンティティに自動的に関連付けます。クエリはどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。注: 正解ごとに1ポイント獲得できます。

Answer Area

```
[ AuditLogs / AzureActivity / AzureDiagnostics ]
| where OperationNameValue in~
("Microsoft.Network/networkSecurityGroups/securityRules/write")
| where ActivityStatusValue == "Succeeded"
| make-series dcount(ResourceId) default=0 on
EventSubmissionTimestamp in range(ago 7d), now (), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
[ | extend / | parse-where / | where ] AccountCustomEntity = Caller
```


正解:



Explanation:

AzureActivity Extend

Explanation = Use AzureActivity because NSG rule changes (operations like Microsoft.Network /networkSecurityGroups/securityRules/write) are re corded in the Azure Activity logs. To automatically associate the security principal (the caller) with a Sentinel entity you create a new column AccountCustomEntity and set it to Caller - that is done with the extend operator.

A completed/cleaned-up versio n of the query (showing the filled choices) would look like:

AzureActivity

| where OperationNameValue in (" Microsoft.Network/networkSecurityGroups/securityRules/write ")

| where ActivityStatusValue == " Succeeded "

| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller

| extend timestamp = todatetime(EventSubmissionTimestamp[0])

| extend AccountCustomEntity = Caller

This produces the anomaly/hunting results grouped by the caller and makes Sentinel treat the Caller value as an account entity for investigations and alert enrichment.

質問**: 167**

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**)**
In Microsoft Defender for Identity, marking accounts as Sensitive instructs the system to monitor those accounts more closely for suspicious activity or lateral movement attempts.
The question describes the goal as configuring several accounts that attackers might exploit. Microsoft Defender for Identity documentation explicitly says:
"Accounts designated as Sensitive are prioritized for monitoring and detection to identify potential compromise attempts." Thus, adding the accounts as Sensitive accounts achieves the goal.
Correct answer: A. Yes

質問**: 168**
Azure Security Center には、テストに使用される 10 台の仮想マシンの抑制ルールがあります。仮想マシンは Windows Server を実行します。
仮想マシンの問題のトラブルシューティングを行っています。
Security Center では、過去 5 日間に仮想マシンによって生成されたアラートを表示する必要があります。
あなたは何をするべきか？
A. 抑制ルールのルール有効期限を変更します。
B. 抑制ルールの状態を無効に変更します。
C. [セキュリティ アラート] ページのフィルターを変更します。
D. 仮想マシン上の Windows イベント ログを表示します。
正解: **(**正解を表示します**)**
A suppression rule in Azure Security Center (Defender for Cloud) prevents specific alerts from appearing in the portal or triggering notifications. When a suppression rule is active, alerts that match its conditions are hidden from view, even though they still occur in the background.
If you need to temporarily view alerts from the suppressed virtual machines - for example, while troubleshooting or verifying detections - you can disable the suppression rule. Microsoft documentation states:
"To temporarily resume visibility of alerts suppressed by a rule, change the rule state to Disabled.
When disabled, the rule no longer hides alerts that meet its conditions." Changing the expiration date (Option A) only controls when the rule automatically stops; it does not immediately restore visibility.
Modifying filters (Option C) won't reveal suppressed alerts, as those are already hidden from query results.
Viewing Windows event logs (Option D) provides raw OS data but not Security Center alert context.
Thus, to see the suppressed alerts for the last five days, you must disable the suppression rule, making B the correct answer.

質問**: 169**
指定された緊急時対応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。

Answer Area

正解:

Explanation:

For a near-real-time (NRT) analytics rule that detects sign-ins by a designated break-glass account, the most direct and performant pattern is to filter SigninLogs by joining to a Microsoft Sentinel watchlist that contains the protected account(s). Sentinel exposes watchlists to KQL through the helper function _GetWatc hlist(' < watchlist-name > ') , which returns a table with standard columns (including SearchKey) plus any custom columns you imported. Using join kind=inner ensures the result set includes only those SigninLogs rows whose UserPrincipalName matches an entry in the watchlist-ideal for alerting on a high-value account without post-filtering.

The completed query is:

SigninLogs | join kind=inner (_GetWatchlist(' breakglass_account ')) on $left.UserPrincipalName == $right.

SearchKey

This approach satisfies the requireme nt to implement an NRT rule for the break-glass account because:

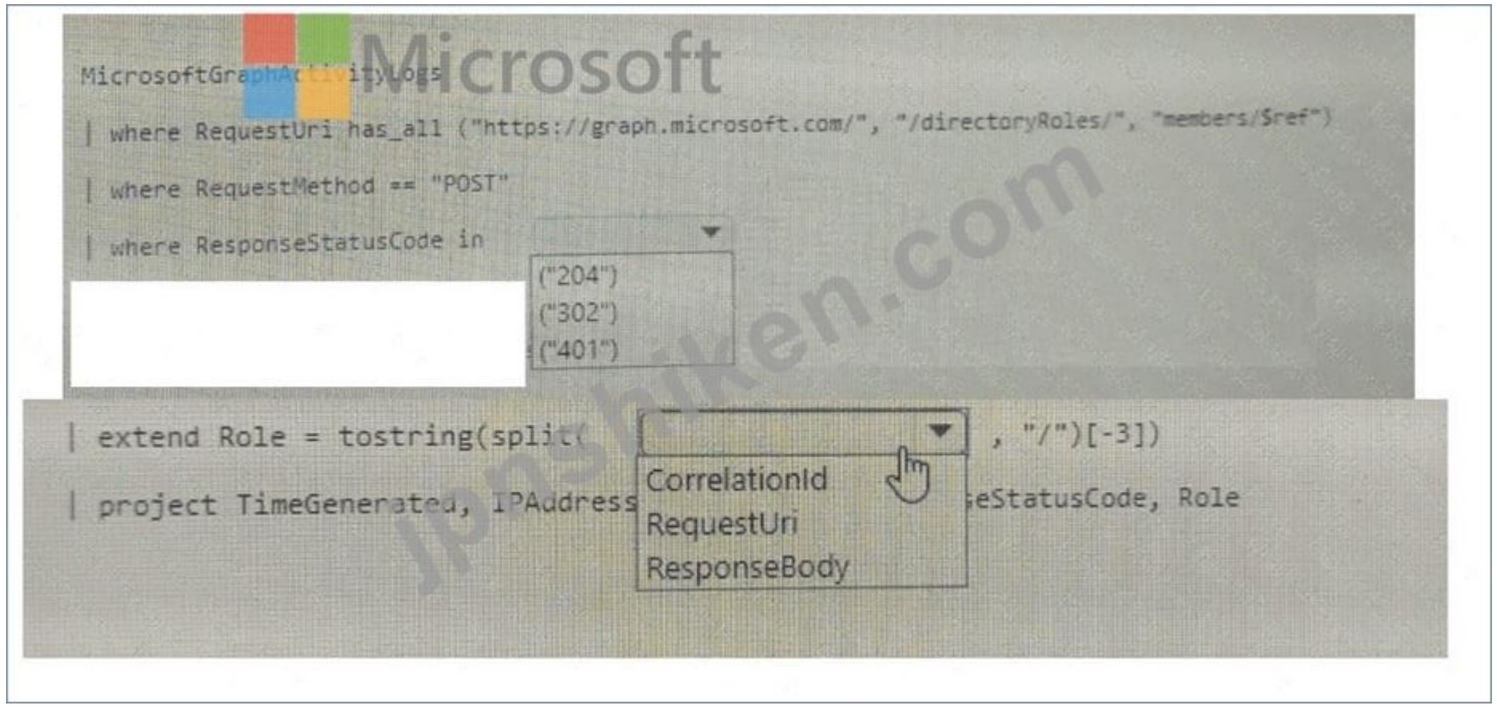
* NRT rules support KQL with joins and watchlists and are optimized for rapid evaluation over fresh data.

* Using a watchlist lets SecOps adjust monitored accounts without editing the rule-minimi zing administrative effort and aligning with least-privilege operations (no extra permissions beyond watchlist management).

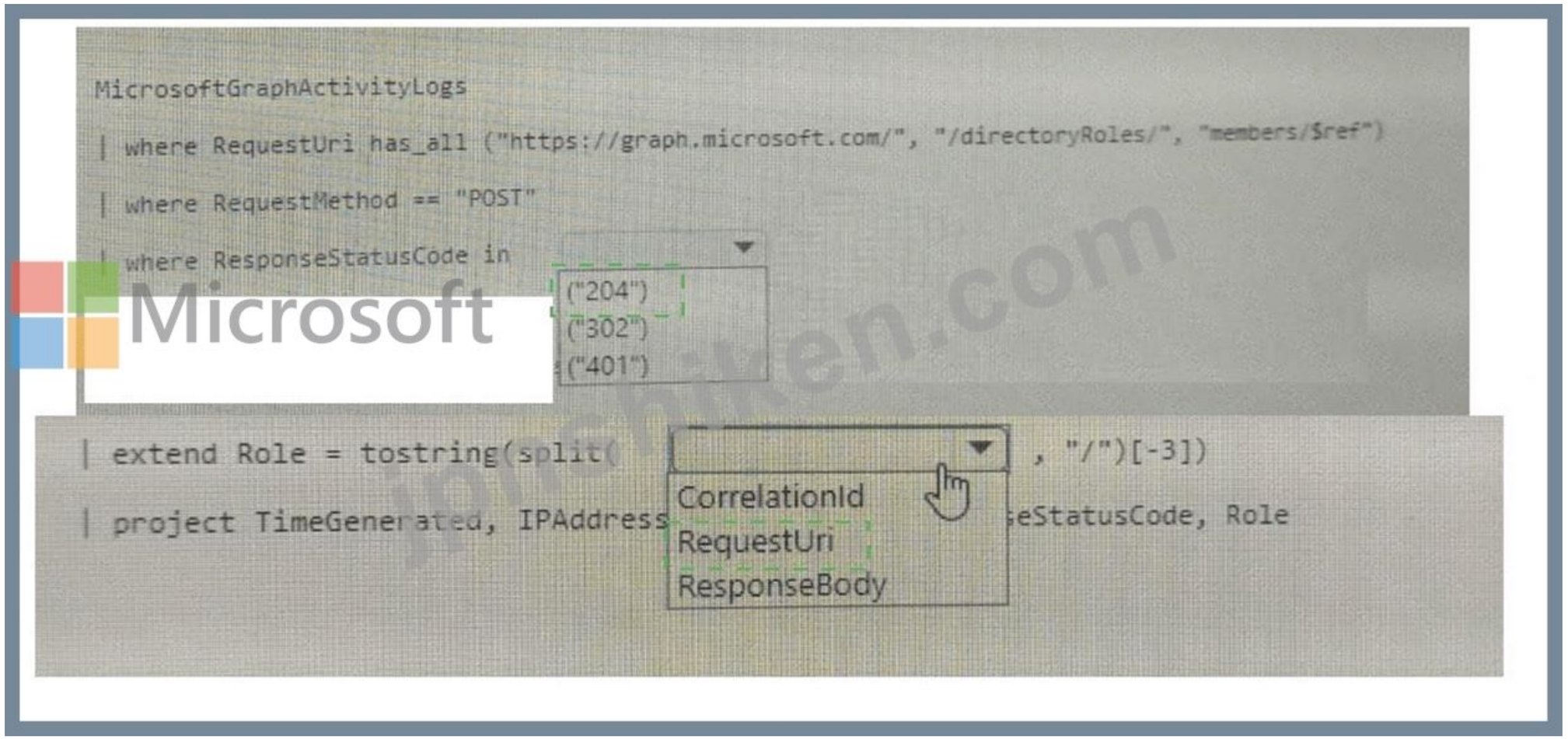
* The inner join pattern reduces noise by returning only matched events, which are then turned into alerts

/incidents by the NRT rule.
Thus, select join and GetWatchlist , and join UserPrincipalName to the watchlist's SearchKey .

質問: **170**
お客様は、contoso.com という名前の Microsoft Entra テナントにリンクされた Microsoft 365 E5 サブスクリプションをお持ちです。
contoso.com における役割の変更を特定するには、Microsoft Graph のアクティビティログを照会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:



Explanation:

Dropdown/Step

Value to Select

where ResponseStatusCode in (...)

(" 204 ")

split([dropdown], " / ")[-3]

RequestUri

To detect Microsoft Graph operations that change role membership , you target POST requests to the directoryRoles ... /members/$ref endpoint. Adding a member to a role via Microsoft Graph is performed with POST /directoryRoles/{role-id}/members/$ref and, on success, Graph returns HTTP 204 No Content .

Therefore, filtering ResponseStatusCode to 204 isolates successful role-assignment events while excluding errors like 401/403 and non-mutating redirects such as 302.

The RequestUri contains the role identifier in the path. For URIs like:

https://graph.microsoft.com/v1.0/directoryRoles/{role-id}/members/$ref

splitting on "/" yields: [https:, , graph.microsoft.com, v1.0, directoryRoles, {role-id}, members, $ref] . The element at index -3 is the {role-id} . Hence, extend Role = tostring(split(RequestUri, " / ")[-3]) correctly extracts the role GUID for reporting.

Putting it together, a concise query is:

MicrosoftGraphActivityLogs

| where RequestUri has_all (" https://graph.microsoft.com/ " , " /directoryRoles " , " members/$ref ")
| where RequestMethod == " POST "
| where ResponseStatusCode in (" 204 ")
| extend Role = tostring(split(RequestUri, " / ")[-3])
| project TimeGenerated, IPAddress, ResponseStatusCode, Role
This returns the timestamp, source IP, success code, and the affected role ID for each successful role- membership addition in your tenant.

質問: **171**
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. workspace1 にソリューションをインストールします。
B. sub1 でプロバイダを登録します。
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 にワークブックを作成します。
正解: **(**正解を表示します**)**
When configuring Microsoft Defender for Cloud (formerly Azure Security Center) to use a specific Log Analytics workspace, you must ensure the Security solution is installed in that workspace so that security events from VMs reporting to the workspace are processed by Defender for Cloud. Registering a provider, creating workflow automations, or creating a workbook do not enable data processing for recommendations
/alerts; installing the solution (now surfaced as the Defender for Cloud agent/solution enablement) does.

質問: **172**
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:

Explanation:

質問: 173

Microsoft Sentinelワークスペースに、Workbook1という名前のカスタムワークブックが含まれています。

SecuntyEvent テーブルに基づいてビジュアルを作成する必要があります。ソリューションは以下の要件を満たす必要があります。

* 過去1週間に取り込まれたセキュリティイベントの数を特定します。

* タイムチャートで日ごとのイベント数を表示する

ワークブック1には何を追加すべきですか？

A. クエリ

B. メトリック

C. グループ

D. リンクまたはタブ

正解: **(正解を表示します)**

In Microsoft Sentinel workbooks , a query visualization is used to retrieve and display data from tables (like SecurityEvent) using Kusto Query Language (KQL) .

To meet the requirements:

* Identify the number of security events ingested in the past week.

* Display the count of events by day in a timechart .

You would add a KQL query control to the workbook, for example:

```
SecurityEvent
| where TimeGenerated > ago(7d)
| summarize Count = count() by bin(TimeGenerated, 1d)
| render timechart
```

* Metric is used for a single numeric value, not a chart.

* Group and Links or tabs are for workbook organization, not visualization.

Correct answer: A. a query

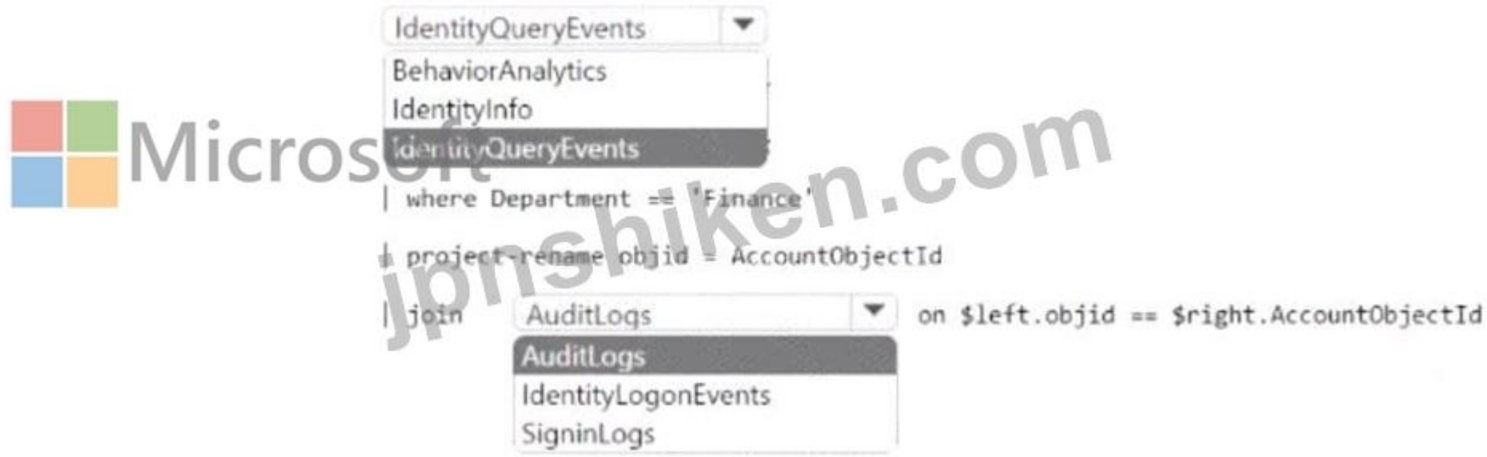
質問: **174**
Azure Sentinel に Playbook があります。
プレイブックをトリガーすると、配布グループに電子メールが送信されます。
配布グループではなくリソースの所有者に電子メールを送信するようにプレイブックを変更する必要があります。
あなたは何をするべきか？
A. パラメータを追加し、トリガーを変更します。
B. カスタム データ コネクタを追加し、トリガーを変更します。
C. 条件を追加し、アクションを変更します。
D. パラメータを追加し、アクションを変更します。
正解: **(正解を表示します)**
When modifying an existing Azure Sentinel playbook (Logic App) to send emails to a dynamic recipient , such as the resource owner , you must make the email destination configurable. This is achieved by adding a parameter in the Logic App.
You then modify the action (the "Send an email" step) to use this parameter as the recipient field instead of a static distribution list. This enables flexibility, allowing the playbook to adapt dynamically based on alert context or Sentinel data fields passed into it.
In Microsoft Sentinel documentation, the best practice for dynamic logic app responses is:
"Use parameters to pass entity information (such as Account, Host, or Owner) from Sentinel alerts into playbooks for dynamic action execution." Hence, the verified answer is D. Add a parameter and modify the action .

質問: **175**
あなたはMicrosoft 365 E5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に登録されています。
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: **(正解を表示します)**
Live Response in Microsoft Defender for Endpoint is a powerful investigative and remediation capability that lets responders interactively run commands on an endpoint, collect files, and perform remediation steps (collect investigation packages, pull files, run scripts, or take forensic artifacts). However, Live Response is an on-demand tool invoked during or after an investigation; it does not by itself provide continuous detection coverage or automatic blocking of artifac ts that a third-party AV missed. The requirement is to ensure devices are protected from malicious artifacts that were undetected by the third-party antivirus . To meet that objective you need capabilities that detect and block artifacts automatically (for example, EDR in block mode which actively blocks/remediates post-breach artifacts even when Defender AV is passive). Live Response helps respond to an identified artifact but does not create the detection and automatic blocking coverage that prevents or re mediate undetected malicious artifacts at scale. Therefore enabling Live Response alone does not meet the stated protection goal.

質問: **176**
お客様のネットワークには、Azure ADと同期するオンプレミスのActive Directoryドメインサービス(AD DS)ドメインが含まれています。
お客様は、Microsoft Defender 365を使用するMicrosoft 365 E5サブスクリプションをご利用中です。貴社の財務部門のユーザーによる、
すべての対話型認証試行を特定する必要があります。
KQLクエリはどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area



正解:

Explanation:

質問**: 177**

Microsoft 365 E5 サブスクリプションと Microsoft Sentinel ワークスペースをお持ちの場合、以下のソースからのデータを組み合わせる KQL クエリを作成する必要があります。

* Microsoft Graph
* Microsoft Entra ID Protection によって検出された危険なユーザー
解決策は、返されるデータ量を最小限に抑える必要があります。クエリはどのように開始すべきでしょうか？
A. MicrosoftGraphActivityLogs
$left.UserId == $right.Id で、種類が leftouter AADRiskyUsers を検索します。
B. MicrosoftGraphActivityLogs
$left.UserId == $right.Id で AADRiskyUsers に参加します
C. MicrosoftGraphActivityLogs
$left.UserId == $right.Id で AADUserRiskEvents に結合します。
D. (MicrosoftGraphActivityLogs、AADUserRiskEvents) 内で検索
正解: **(**正解を表示します**)**
To combine Microsoft Graph activity logs with Microsoft Entra ID Protection risky users , while minimizing data volume, you use the lookup kind=leftouter operator.
Microsoft documentation explains:
"Use lookup (instead of join) when you need to enrich a large dataset with a small lookup table to minimize data returned."
* MicrosoftGraphActivityLogs provides user activity records.
* AADRiskyUsers lists users detected as risky by Entra ID Protection.
* A leftouter lookup ensures all Microsoft Graph activity entries are kept, while only matching risky user info is appended - reducing output volume compared to a full join .
# Correct Answer: A. MicrosoftGraphActivityLogs lookup kind=leftouter AADRiskyUsers on $left.
UserId == $right.Id

質問: **178**
お客様は、Microsoft Defender for Endpointを使用するAzureサブスクリプションをお持ちです。
ユーザーが指定したIPアドレスとURLの範囲を許可またはブロックできることを確認する必要があります。
Microsoft 365 Defender ポータルのエンドポイント設定にある高度な機能で、最初に有効にすべき機能は何ですか？
A. ブロックモードのエンドポイント検出および応答 (EDR)
B. カスタムネットワークインジケーター
C. ウェブコンテンツフィルタリング
D. サーバーからのライブ応答
正解: **(**正解を表示します**)**
In Microsoft Defender for Endpoint , before administrators can allow or block user-specified IPs or URLs, the feature "Custom network indicators" must be enabled under Advanced Features in the Microsoft 365 Defender portal .
This capability allows defining Indicators of Compromis e (IoCs) at the network level to enforce allow
/block decisions for specific domains, URLs, or IP ranges. Once enabled, Defender for Endpoint agents enforce these network indicators across managed endpoints.
Other features like EDR in block mode or Web cont ent filtering provide automatic blocking, not manual IP
/URL control.
Correct Answer: B. custom network indicators