Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://tw.fast2test.com

高效的考試材料是最高通過率的考試題庫

Exam : **SC-200**

Title : Microsoft Security Operations Analyst

Vendor : Microsoft

Version : DEMO

NO.1 You need to complete the query for failed sign-ins to meet the technical requirements.
Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center

B. Activity log in Azure

C. Azure Advisor

D. the query windows of the Log Analytics workspace

Answer: D

Explanation:

To complete the KQL query against the BehaviorAnalytics table, 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 pane, 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 type 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 autocomplete to insert the correct column name.

Topic 1, Contoso Ltd

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 in 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 the 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 environment, 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

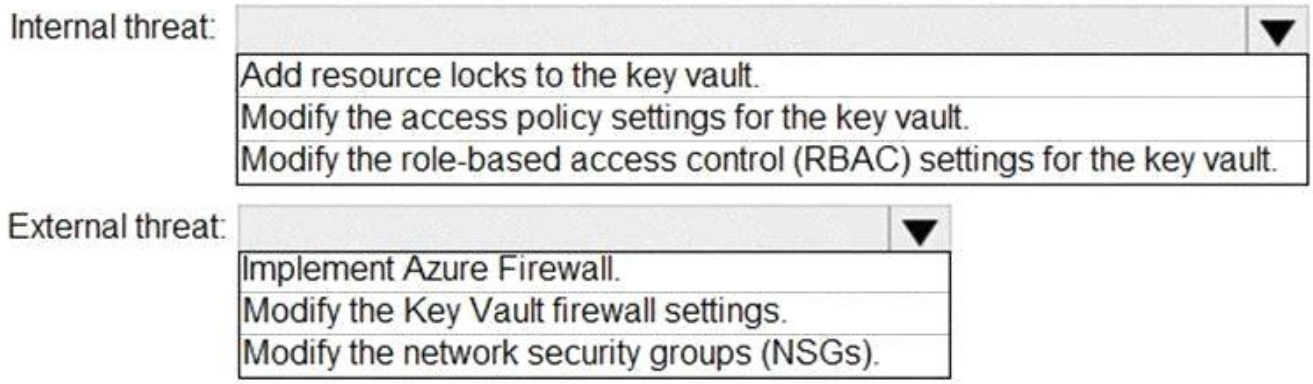
A company named Contoso Ltd. has a main office and five branch offices located throughout North

America.
The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.
Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
* Receive alerts if an Azure virtual machine is under brute force attack.
* Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
* Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
* Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
* Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == " FailedLogOn "
| where _____ == True

NO.2 You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

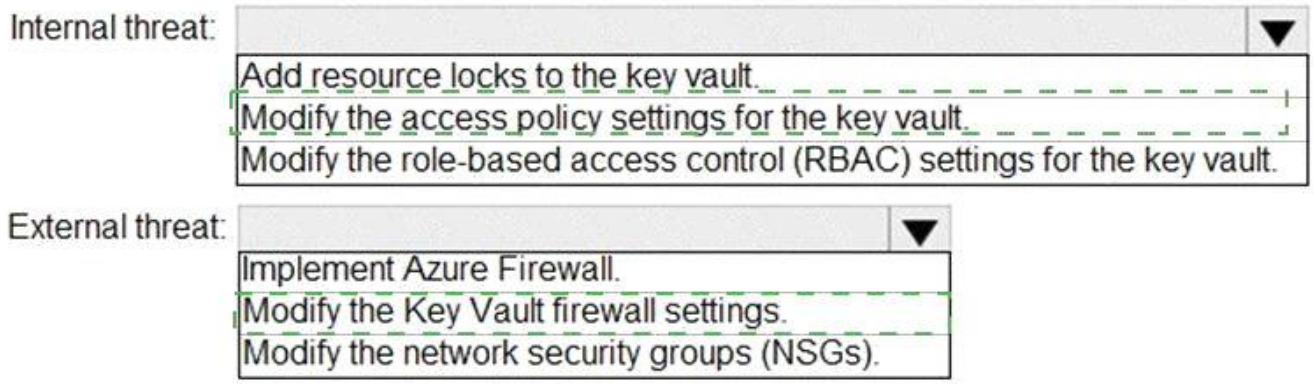
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:
Internal threat: Modify the access policy settings for the key vault.
External threat: Modify the Key Vault firewall settings.
For internal threats involving a potential compromise of Fabrikam's own Azure AD applications, the most direct and least disruptive remediation is to modify the Key Vault access policies (or RBAC assignments, if RBAC for Key Vault data-plane is in use) to immediately remove or reduce the compromised service principal's permissions (Get/List/Decrypt/Sign/Wrap). Microsoft guidance for Key Vault access emphasizes least privilege and promptly revoking credentials or app permissions when compromise is suspected. Access policies (or data-plane RBAC) govern which identities can access secrets, keys, and certificates; adjusting these stops further data-plane actions by the compromised app. "Resource locks" protect against deletion or configuration changes at the management plane, but they do not remove a compromised identity's ability to read or use vault objects, so they are not an appropriate first response for this scenario.
For external threats , Microsoft recommends hardening Key Vault firewall and networking : restrict public network access, allow only required IPs, use virtual network rules, and prefer private

endpoints. Key Vault includes a built-in firewall for IP and VNet ACLs; tuning these controls reduces exposure to the public internet and blocks unauthorized traffic. NSGs apply to IaaS subnets/nics and don't directly secure the public Key Vault endpoint. Azure Firewall can add perimeter control, but it is not necessary for remediating a specific Key Vault Defender alert; the most effective and immediate remediation is tightening the Key Vault firewall settings to limit external access pathways.

NO.3 The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive

B. marketing

C. security

D. sales

Answer: B

Explanation:

As outlined in Microsoft's official Defender for Office 365 documentation, this service provides comprehensive protection against threats targeting Microsoft 365 collaboration tools-such as SharePoint Online , OneDrive for Business , and Microsoft Teams . The marketing team uses SharePoint Online for vendor collaboration and has experienced incidents in which vendors uploaded malicious files. Microsoft Defender for Office 365 specifically addresses this scenario through fea tures like Safe Attachments and Safe Links , which automatically scan uploaded or shared files for malware and block access to harmful content.

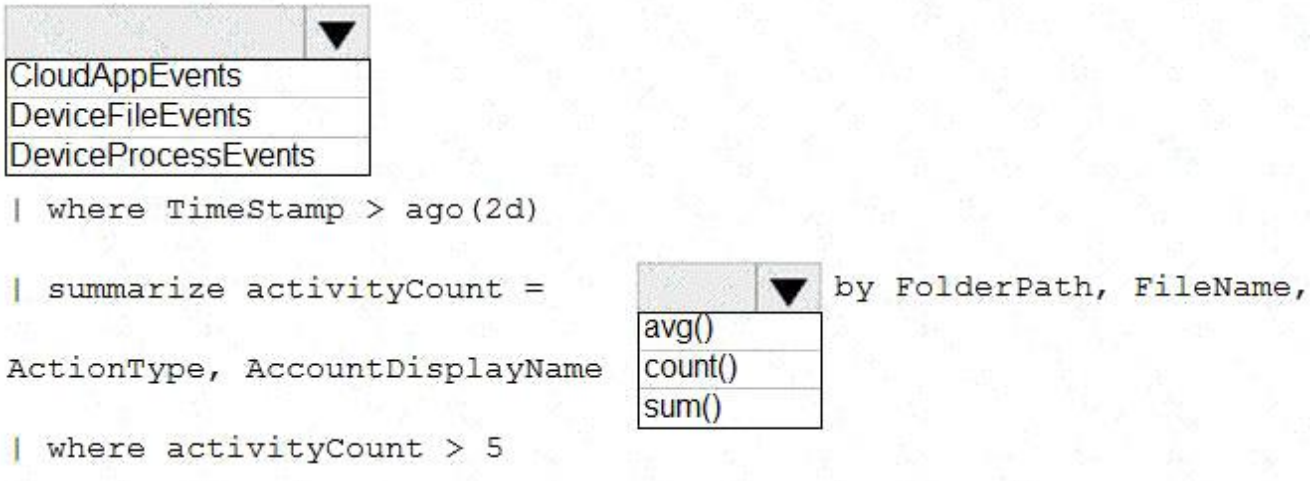
When a vendor uploads a file to SharePoint Online, Defender for Office 365 inspects the file in real time within a virtual sandbox environment before allowing users to open or share it. If malware is detected, the system quarantines or removes the file and notifies administrators. These detection and remediation capabilities prevent infection propagation, protect sensitive marketing data, and maintain compliance with Contoso's security posture.

By leveraging Defender for Office 365, Contoso's marketing team can continue external collaboration safely, ensuring that all uploaded files are scanned and validated before internal access-thereby resolving their specific malware-related issue.

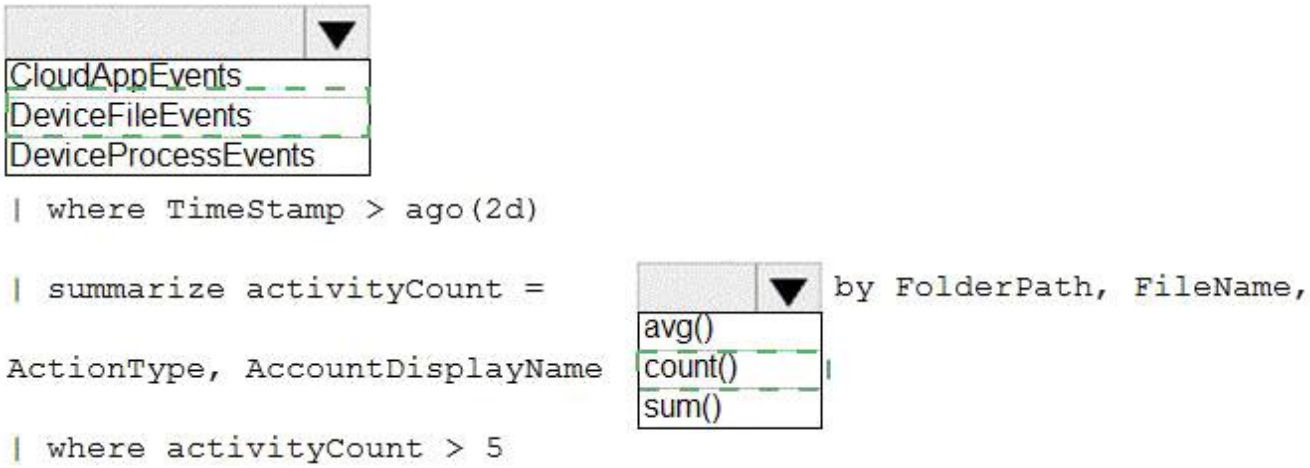
NO.4 You need to create an advanced hunting query to investigate the executive team issue.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



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 typical 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 to 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 DeviceProcessEvents 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()

NO.5 You need to remediate active attacks to meet the technical requirements.
What should you include in the solution?
A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure Functions

D Azure Sentinel livestreams

Answer: B

Explanation:

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 changes- 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 playbook 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 or 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 integrate 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 remediate 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 response capabilities.

NO.6 The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive

B. sales

C. marketing

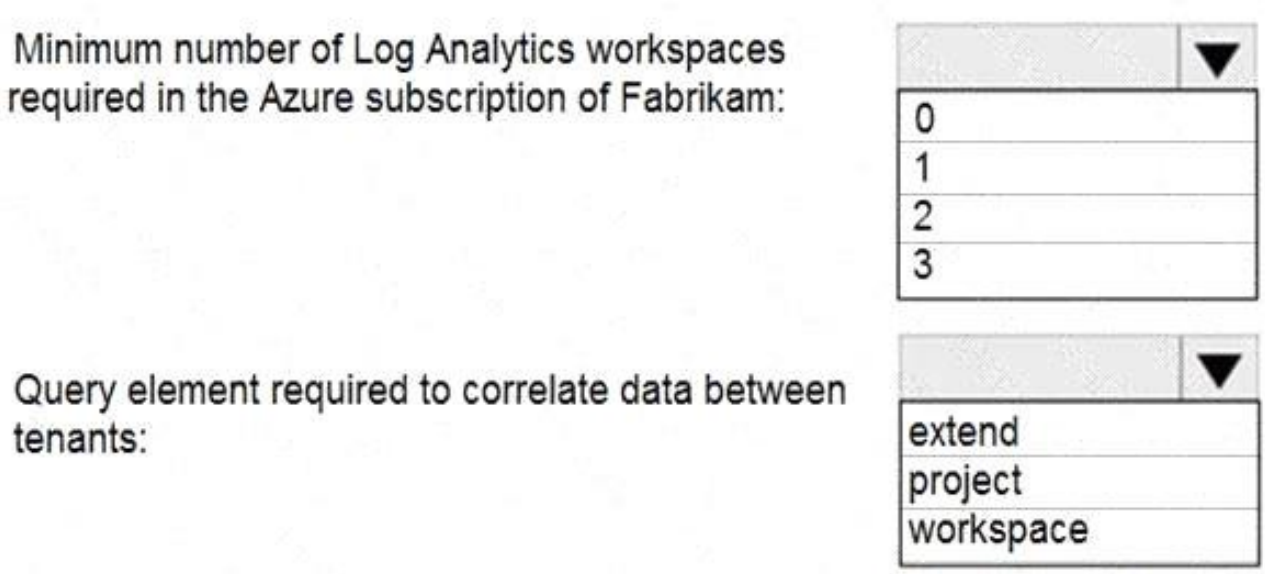
Answer: B

Explanation:

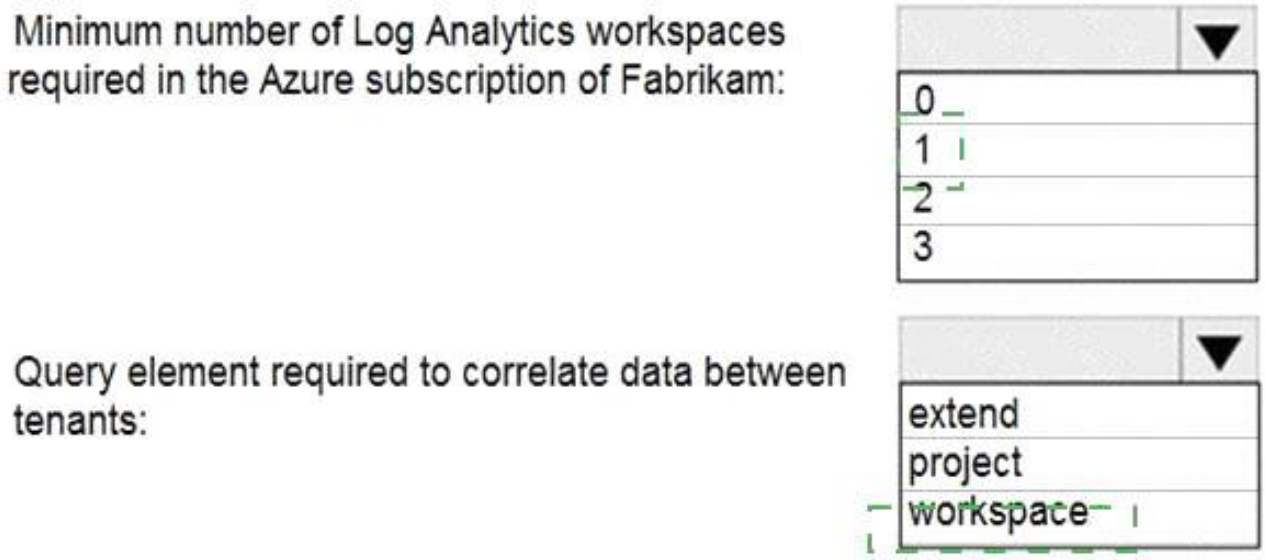
According to Microsoft Security Operations documentation, Microsoft Defender for Endpoint is designed to protect endpoint devices-including Windows, macOS, Android, and iOS -against cyberattacks through advanced behavioral analysis, threat intelligence, and automated investigation and remediation. In the given case study, the sales team exclusively uses iOS devices and has previously experienced attacks while exchanging files using third-party applications. These unmanaged file-sharing methods exposed the team to malware, phishing, and data leakage threats. By implementing Microsoft Defender for Endpoint on iOS, Contoso can apply unified endpoint protection across all mobile devices. Defender for Endpoint's mobile threat defense (MTD) capabilities detect malicious apps, risky network connections, jailbroken devices, and phishing attempts. It also integrates with Microsoft Intune for compliance enforcement and conditional access-ensuring only secure, compliant devices can access corporate resources. This directly mitigates the security challenges faced by the sales team while minimizing manual investigation effort through automated response.

Therefore, the issue affecting the sales team (mobile device attacks and unsafe file transfers) can be effectively resolved using Microsoft Defender for Endpoint .

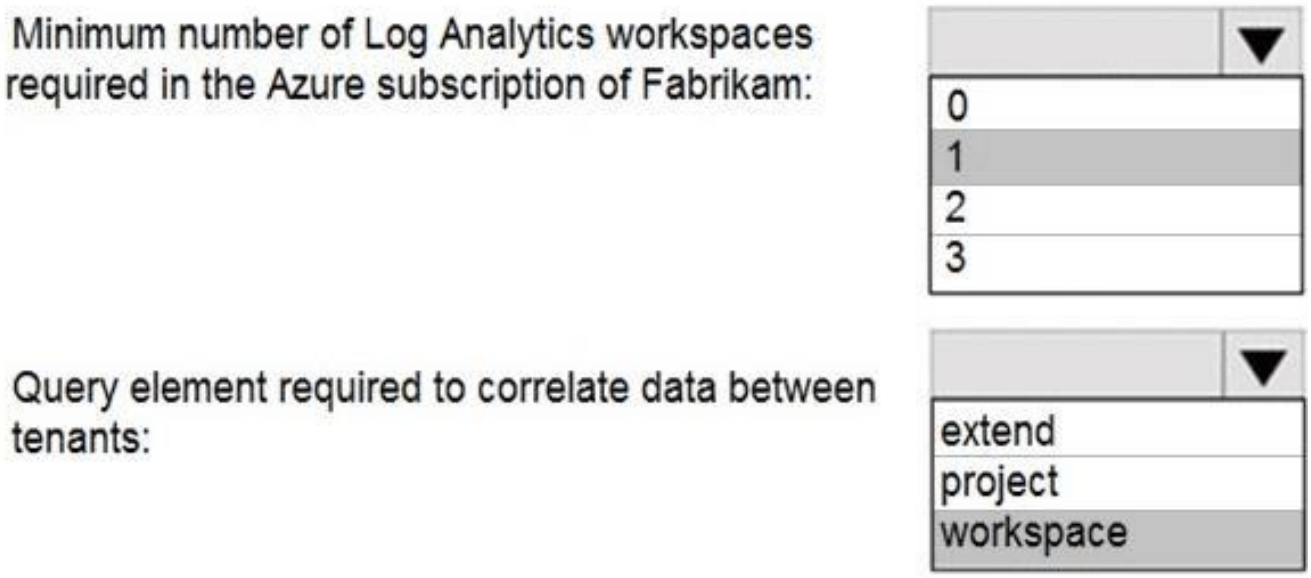
NO.7 You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



In Microsoft Sentinel (built on Azure Monitor Logs), analytics and hunting queries are executed within a Log Analytics workspace . To run Sentinel queries for Fabrikam, the tenant must have at least one workspace (with Sentinel enabled) in its subscription to host rules, incidents, hunting queries, and workbooks. Sentinel's cross-workspace/tenant capability is provided by cross-resource queries in Kusto Query Language (KQL).
The key construct for reaching outside the current workspace is the workspace() function, which lets you reference another Log Analytics workspace by name or resource ID-even across subscriptions or tenants when proper permissions (often via Azure Lighthouse or guest access) are in place.
Typical correlation looks like:
union workspace(' Fabrikam-WS ').SecurityEvent, workspace(' Contoso-WS ').SecurityEvent | ...
Here, workspace() is the required element to bring together data sets from multiple tenants; operators like extend and project only shape columns and do not establish cross-tenant scope.
Therefore, to meet the requirements with minimal overhead: Fabrikam needs one workspace to host its Sentinel content, and you use workspace() in your KQL to correlate Contoso and Fabrikam data.

NO.8 You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender

C. Azure Firewall

D. Azure Application Gateway

Answer: B

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 indicate 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 triggered 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 Defender 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.
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 in 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 the 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 environment, 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
Litware 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.

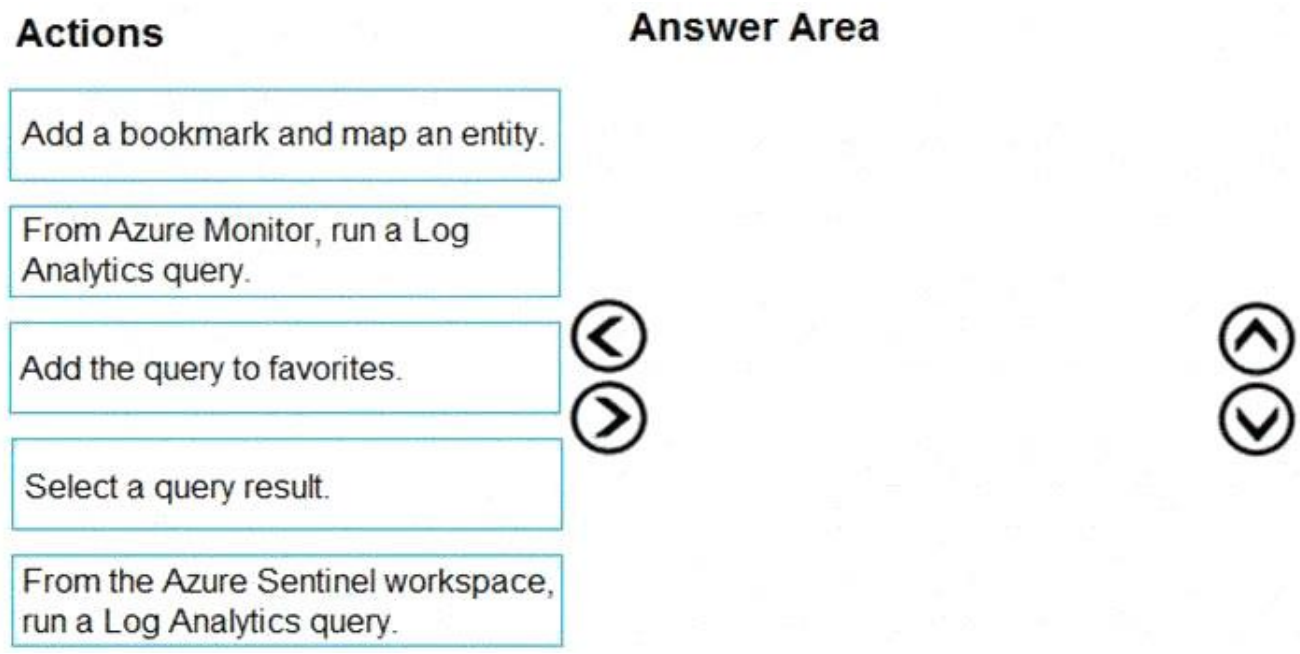
Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems
Cloud App Security frequently generates 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 using 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 stored 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 Microsoft 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.

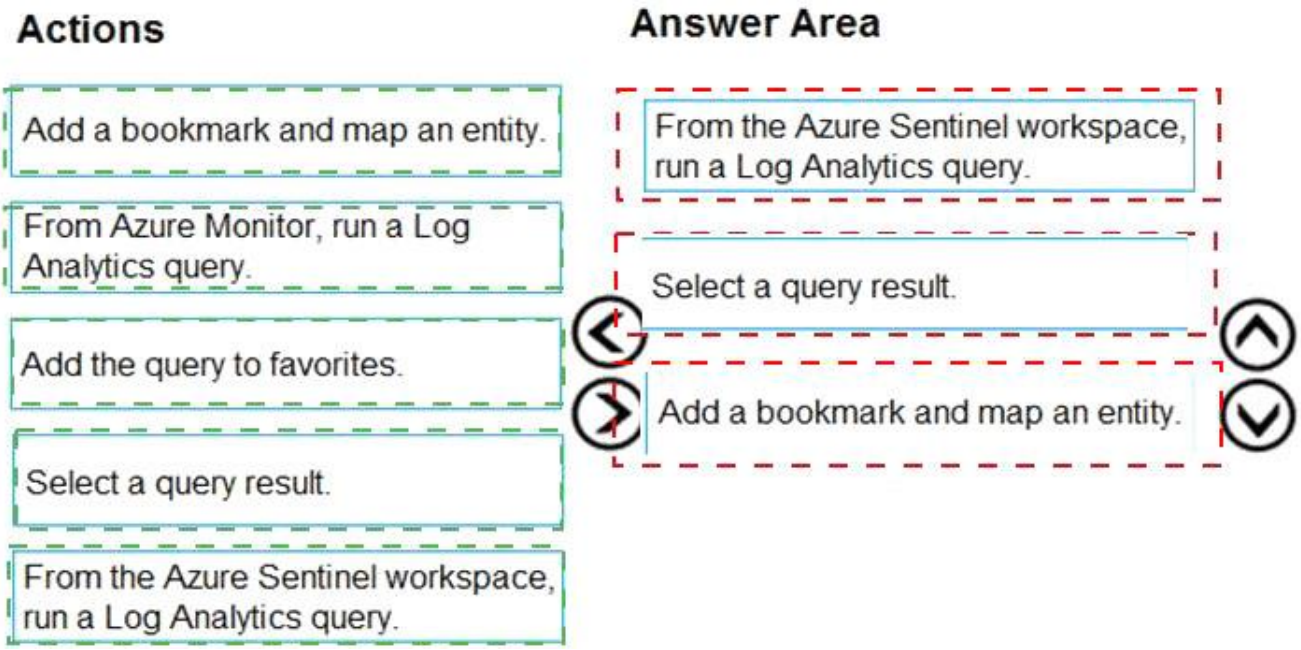
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NO.9 Which rule setting should you configure to meet the Microsoft Sentinel requirements?
A. From Set rule logic, turn off suppression.
B. From Analytic rule details, configure the tactics.
C. From Set rule logic, map the entities.
D. From Analytic rule details, configure the severity.
Answer: C
Explanation:
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.

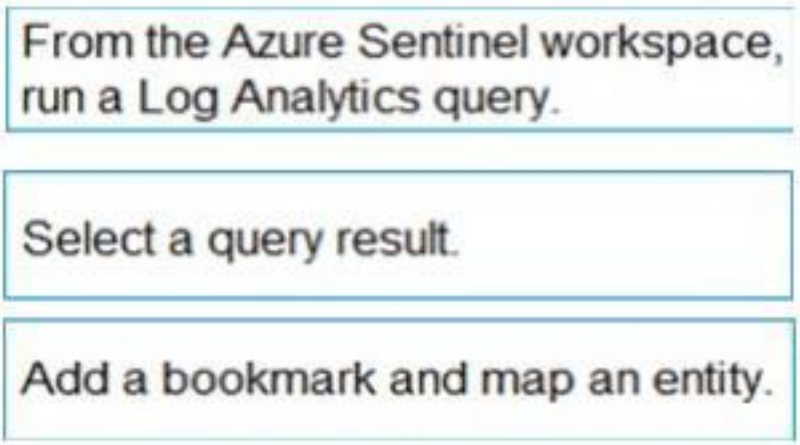
NO.10 You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Answer:



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 mapped 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.

NO.11 You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A. Automation Operator

B. Automation Runbook Operator

C. Azure Sentinel Contributor

D. Logic App Contributor

Answer: D

Explanation:
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.

NO.12 You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center

B. Cloud App Security anomaly detection policies

C. Advanced features from Settings in Microsoft Defender Security Center

D. the Cloud Discovery settings in Cloud App Security

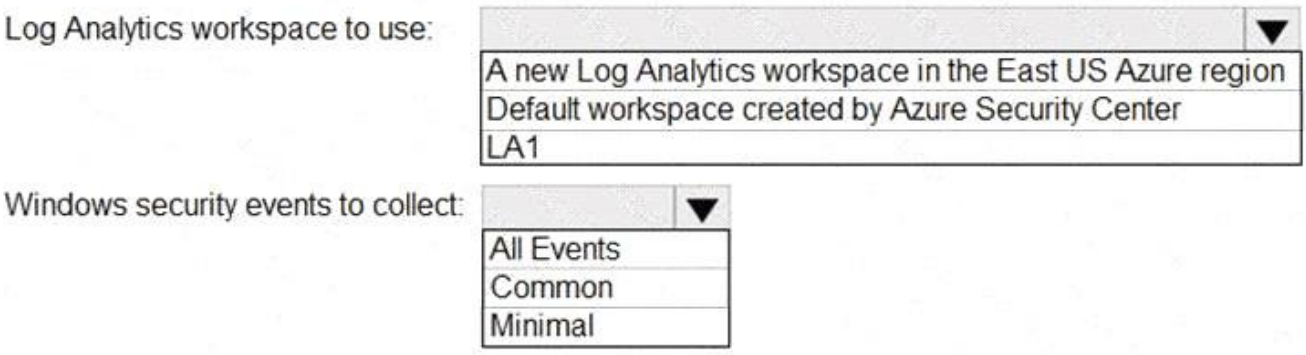
Answer: C D

Explanation:
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 .

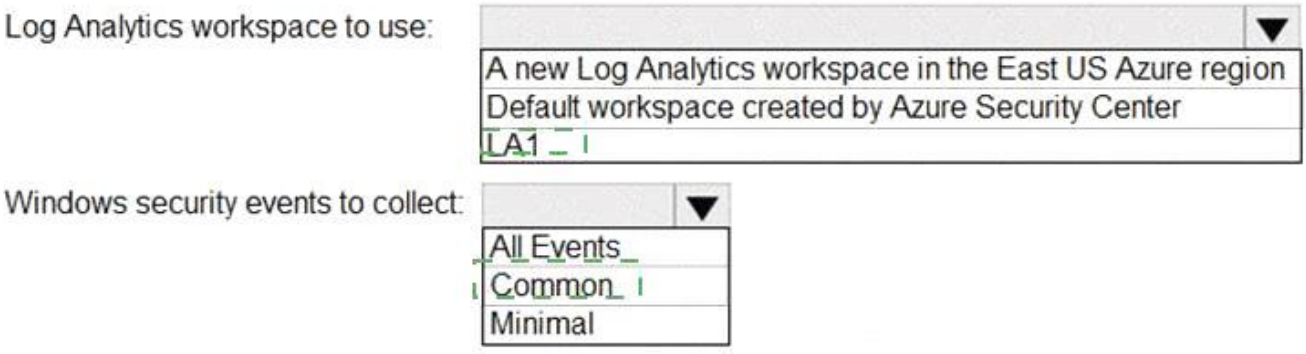
NO.13 You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

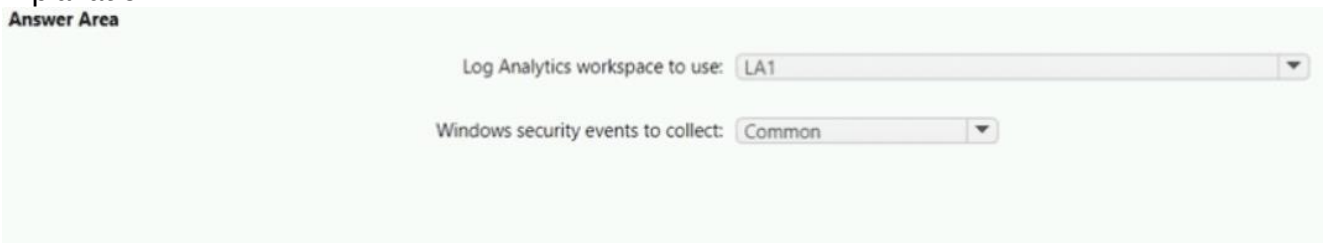


Answer:

Answer Area



Explanation:



According to Microsoft Defender for Cloud (formerly Azure Security Center) documentation, when integrating servers and virtual machines for security monitoring, the Defender for Cloud data is stored and analyzed in a Log Analytics workspace . Microsoft best practices recommend using an existing workspace when one is already deployed for centralized log collection-especially if it already gathers telemetry from Azure and on-premises resources.
In this case, the existing workspace LA1 already "contains logs and metrics collected from all Azure resources and on-premises servers." This satisfies the business requirement of "all servers must send logs to the same Log Analytics workspace." Creating a new workspace would violate the cost-minimization and centralization requirements. Therefore, LA1 is the correct workspace to use.
For the Windows security events collection setting, Defender for Cloud offers three levels:
* Minimal - collects essential security events only (insufficient for comprehensive monitoring).
* Common - collects a balanced set of security-related events (such as account logon, privilege use, and object access), recommended by Microsoft for most environments.
* All Events - collects every possible security event, which increases data ingestion cost and is typically used only for high-security or regulated environments.
Because Litware Inc. must minimize cost while ensuring a full audit trail of user activities , the Common level provides the optimal balance of visibility and cost efficiency.
Therefore, based on Microsoft Defender for Cloud configuration guidelines:
Log Analytics workspace to use: LA1
Windows security events to collect: Common

NO.14 You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

A. From Set rule logic, turn off suppression.

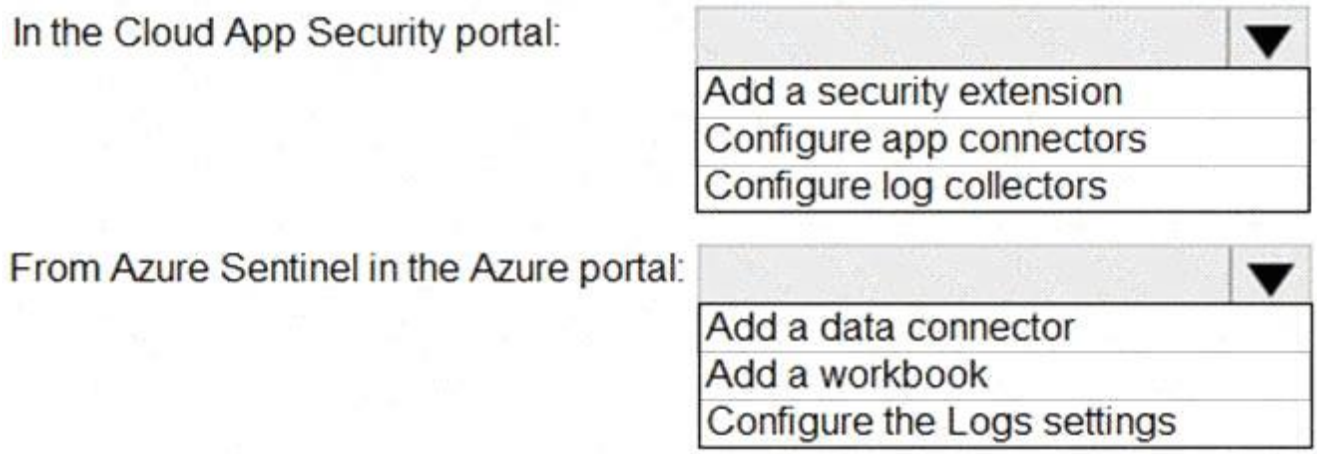
B. From Analytics rule details, configure the tactics.

C. From Set rule logic, map the entities.

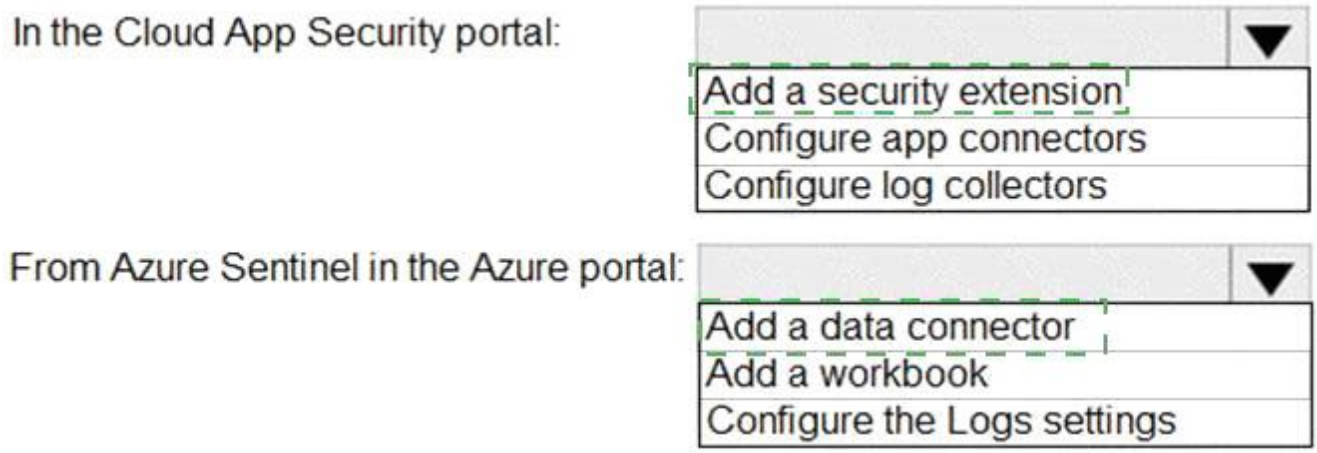
D. From Analytics rule details, configure the severity.

Answer: C
Explanation:
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.

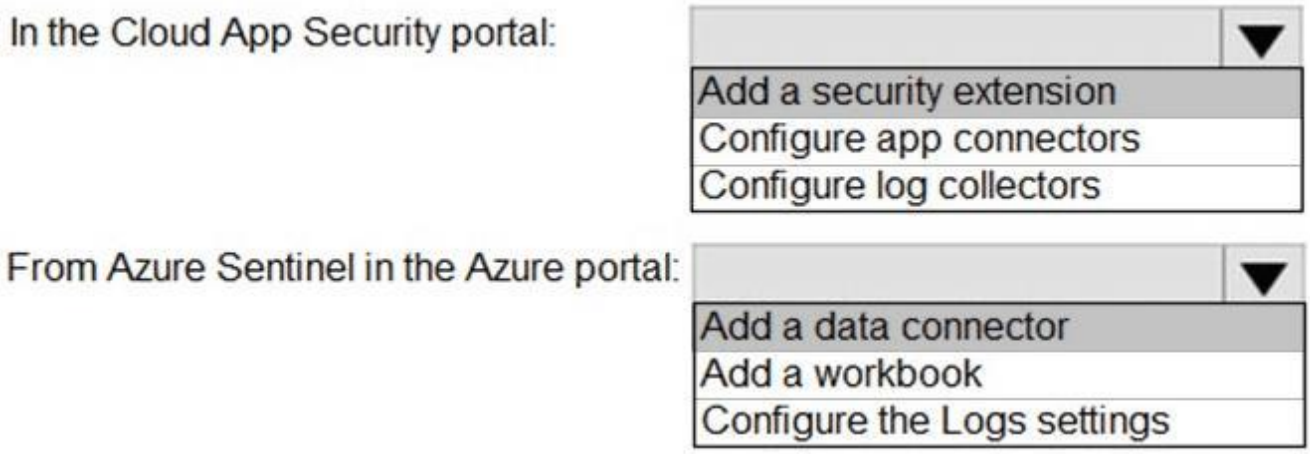
NO.15 You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



To integrate Microsoft Defender for Cloud Apps (MCAS) with Microsoft Sentinel , Microsoft's official SecOps and Sentinel documentation specifies a two-step configuration process.
* In the Defender for Cloud Apps portal - You add a security extension to enable integration with external SIEM platforms. This action allows MCAS to forward its alerts, activities, and discovered app telemetry to other Microsoft or third-party security platforms. By adding the security extension , Defender for Cloud Apps is authorized to send data streams and alerts to Microsoft Sentinel through a supported API connection.
* In Microsoft Sentinel (Azure portal) - You then add a data connector . Data connectors in Sentinel are predefined integration pipelines that bring in telemetry from Microsoft or external security solutions. The Microsoft Defender for Cloud Apps connector specifically ingests MCAS alerts and audit logs into Sentinel, where they can be correlated with other Microsoft Defender XDR signals, enabling unified detection and investigation across identity, endpoint, and cloud layers.
This integration approach adheres to Microsoft's principle of minimizing administrative effort by using native connectors rather than custom ingestion or log collector configurations. Once connected, Sentinel automatically normalizes MCAS alerts into its SecurityAlert and CloudAppEvents tables for rule creation, playbook automation, and incident correlation.
Therefore, the verified correct configuration is:
* Defender for Cloud Apps: Add a security extension
* Sentinel: Add a data connector

NO.16 You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.
Which policy should you modify?
A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel
D. Risky sign-in
Answer: C
Explanation:
The requirement states that Cloud App Security (Defender for Cloud Apps) must determine whether a user's connection is anomalous based on tenant-level patterns , and the current false positives occur when users connect through two office egress points at the same time. These symptoms align with the Impossible travel anomaly detection policy, which learns normal sign-in geolocation patterns and flags sign-ins from distant locations within an unrealistically short time window. To meet the

requirement and reduce false positives, you modify the Impossible travel policy settings-such as excluding trusted corporate IP ranges/VPN egress points and tuning sensitivity-so detections better reflect tenant-wide behavior rather than isolated user hops via different office exits. Policies like Activity from anonymous/suspicious IP addresses rely on threat-intel lists of anonymizers or known-bad sources and don't address the "two-office" scenario. Risky sign-in is part of Azure AD Identity Protection, not the MCAS anomaly policy to tune here. Thus, the policy to modify is Impossible travel .

NO.17 You need to restrict cloud apps running on CUENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Cloud Discovery settings in Microsoft Defender for Cloud Apps

B. the Onboarding settings from Device management in Settings in Microsoft 365 Defender portal

C. Microsoft Defender for Cloud Apps anomaly detection policies

D. Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal

Answer: A D

Explanation:

To restrict cloud apps running on CLIENT1 (a Windows 10 endpoint) in compliance with Microsoft Defender for Endpoint (MDE) requirements, you must integrate Microsoft Defender for Endpoint with Microsoft Defender for Cloud Apps (formerly Cloud App Security) using Cloud Discovery . This integration enables the blocking of unsanctioned cloud apps through the endpoint's network protection capabilities.

According to Microsoft Defender for Cloud Apps documentation , Cloud Discovery uses traffic data from Defender for Endpoint to identify and manage the use of shadow IT. The relevant steps include:

1# # Enable advanced features in Microsoft Defender for Endpoint (M365 Defender portal # Settings # Endpoints # Advanced features).

You must enable the following advanced features:

* Microsoft Defender for Cloud Apps integration
* Network protection (in block mode)
* Custom network indicators (if applicable) These options allow Defender for Endpoint to share telemetry and enforce app restrictions received from Defender for Cloud Apps.

2# # Configure Cloud Discovery settings in Microsoft Defender for Cloud Apps.

In the Defender for Cloud Apps portal, Cloud Discovery must be configured to receive continuous reports from Defender for Endpoint devices. Within these settings, you define sanctioned and unsanctioned applications. Once an app is marked as unsanctioned , Defender for Endpoint enforces blocking on all onboarded devices (like CLIENT1).

This two-part configuration ensures that MDE enforces the blocking of unsanctioned cloud applications discovered through Cloud App Security telemetry, fulfilling the business requirement that "All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint."

NO.18 You need to implement the Azure Information Protection requirements. What should you configure first?

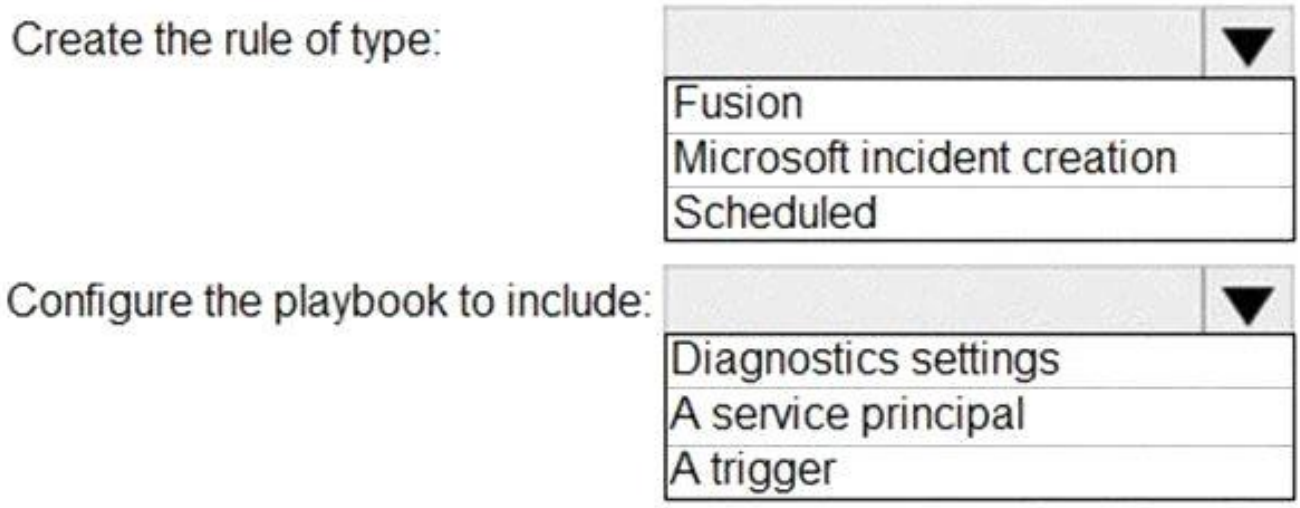
A. Device health and compliance reports settings in Microsoft Defender Security Center

B. scanner clusters in Azure Information Protection from the Azure portal

C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center
Answer: D
Explanation:
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 Security 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 labeled 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 inventory 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.

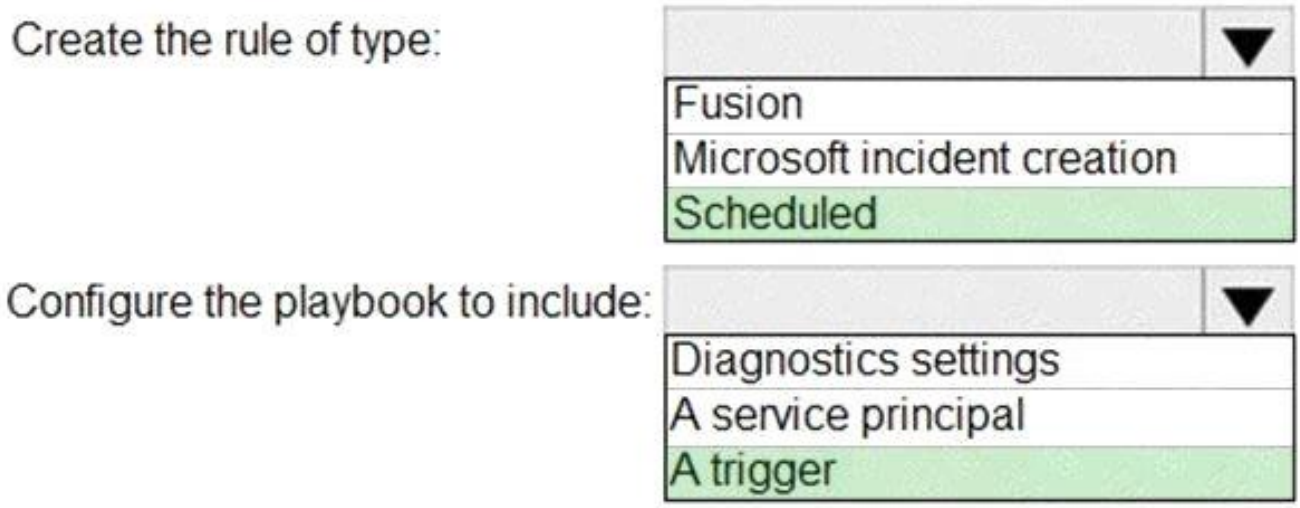
NO.19 You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



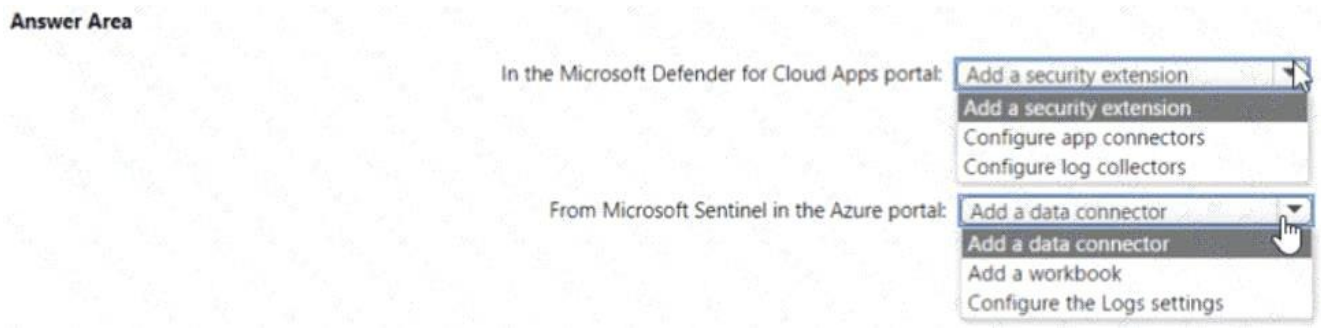
Answer:

Answer Area



According to Microsoft Security Operations (SecOps) and Azure Sentinel documentation, when you need to create an analytics rule that executes a custom KQL query and automatically initiates a playbook , the correct configuration is to create a Scheduled rule and ensure the playbook includes a trigger .
Here's why:
* A Scheduled analytics rule in Microsoft Sentinel (Microsoft Defender XDR portal) is designed for running custom KQL queries at defined intervals (for example, every hour or every few minutes) to detect specific patterns of suspicious activity. When the rule's conditions are met, Sentinel generates alerts that can automatically trigger a playbook for response and automation.
* A playbook in Sentinel is an Azure Logic App that automates responses to incidents or alerts. To connect a playbook to an analytics rule, it must include a trigger -specifically, the "Microsoft Sentinel Alert" or "Incident trigger." This allows the rule to start the playbook automatically when the defined condition is met.
The other options are incorrect because:
* Fusion rules are built-in and use Microsoft's machine learning to correlate signals automatically; they can't be used for custom queries.
* Microsoft incident creation rules are also built-in and handle alert-to-incident grouping logic, not custom query execution.
* A service principal would be needed for permissions (e.g., admin1 configuring playbooks), but not inside the playbook itself.
* Diagnostics settings apply to log collection and retention, not rule automation.
Therefore, based on Microsoft Sentinel best practices and documentation:
Create the rule of type: Scheduled
Configure the playbook to include: A trigger

NO.20 You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Explanation:

To integrate Microsoft Defender for Cloud Apps (MCAS) with Microsoft Sentinel , Microsoft's official SecOps and Sentinel documentation specifies a two-step configuration process.

* In the Defender for Cloud Apps portal - You add a security extension to enable integration with external SIEM platforms. This action allows MCAS to forward its alerts, activities, and discovered app telemetry to other Microsoft or third-party security platforms. By adding the security extension , Defender for Cloud Apps is authorized to send data streams and alerts to Microsoft Sentinel through a supported API connection.
* In Microsoft Sentinel (Azure portal) - You then add a data connector . Data connectors in Sentinel are predefined integration pipelines that bring in telemetry from Microsoft or external security solutions. The Microsoft Defender for Cloud Apps connector specifically ingests MCAS alerts and audit logs into Sentinel, where they can be correlated with other Microsoft Defender XDR signals, enabling unified detection and investigation across identity, endpoint, and cloud layers.

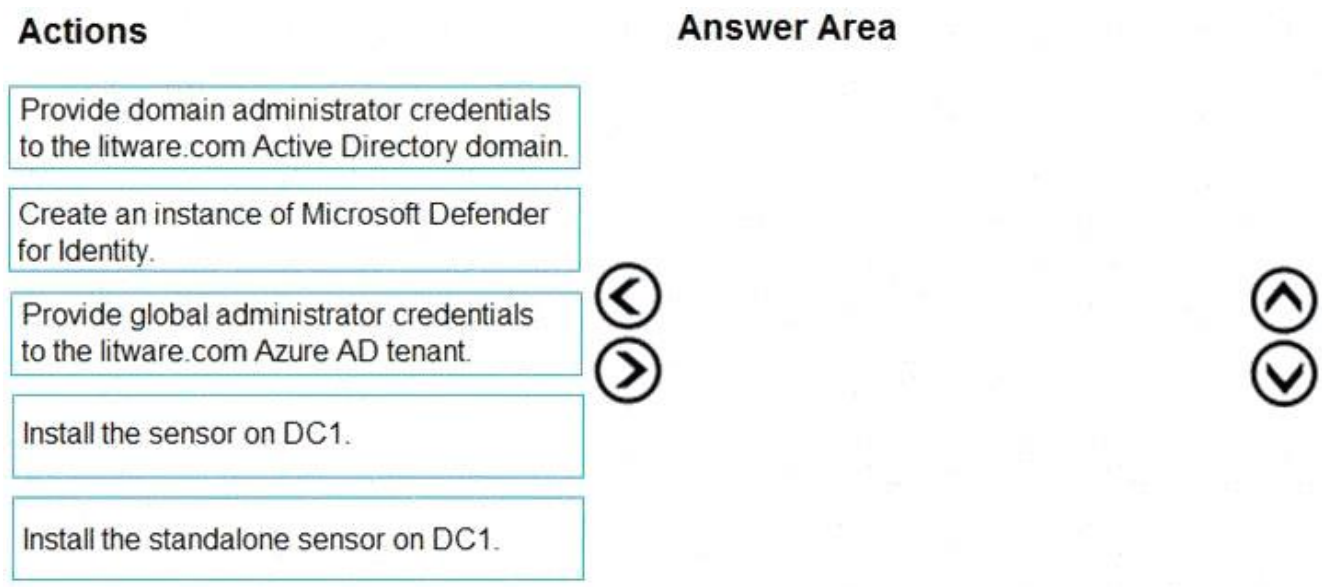
This integration approach adheres to Microsoft's principle of minimizing administrative effort by using native connectors rather than custom ingestion or log collector configurations. Once connected, Sentinel automatically normalizes MCAS alerts into its SecurityAlert and CloudAppEvents tables for rule creation, playbook automation, and incident correlation.

Therefore, the verified correct configuration is:

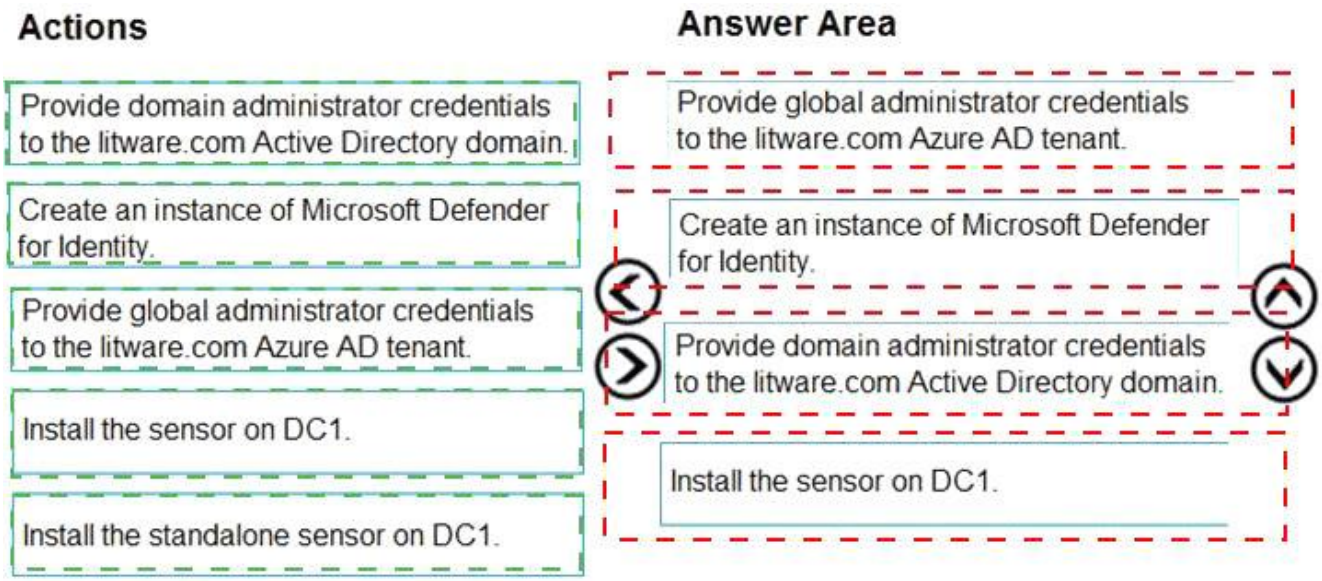
* Defender for Cloud Apps: Add a security extension
* Sentinel: Add a data connector

NO.21 You need to configure DC1 to meet the business requirements.

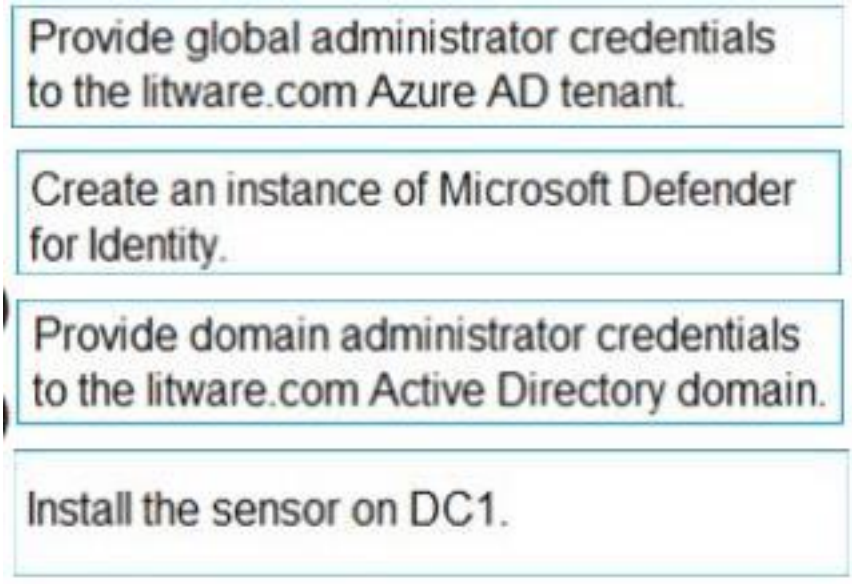
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



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.

NO.22 You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.
Which policy should you modify?

A. Activity from suspicious IP addresses

B. Risky sign-in

C. Activity from anonymous IP addresses

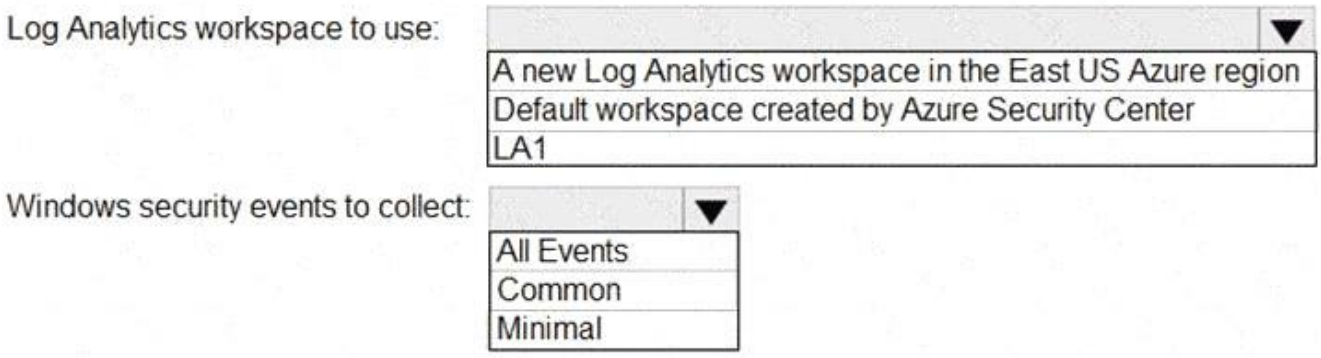
D. Impossible travel

Answer: D

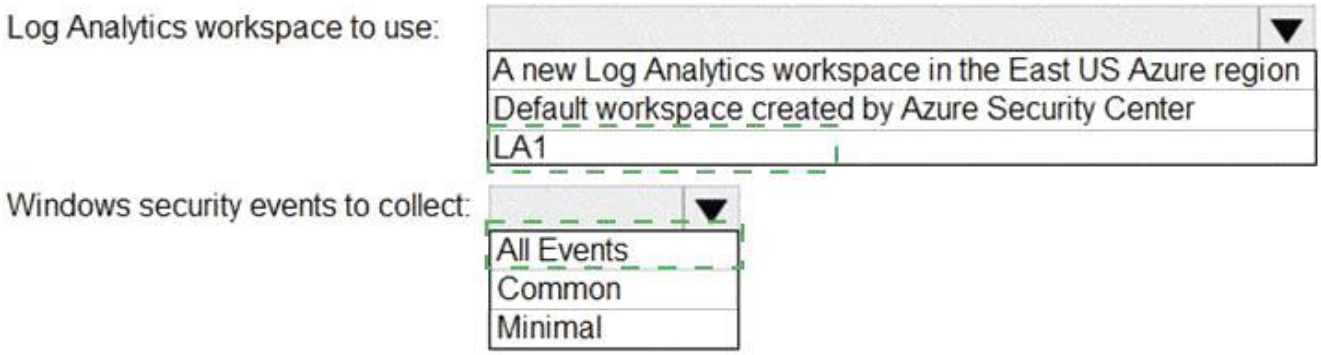
Explanation:
The problem described in the case study states that "Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously." This behavior is commonly associated with the
"Impossible travel" anomaly detection policy in Microsoft Defender for Cloud Apps .
According to Microsoft documentation, the "Impossible travel" policy detects when a user signs in from two locations that are geographically distant within an unrealistic timeframe. However, in multi-office environments (such as Boston and Seattle) or when VPN connections are used, this policy can

frequently trigger false positives , since it may misinterpret legitimate connections as anomalous. Microsoft recommends adjusting the impossible travel detection policy to account for trusted IP ranges, known locations, or VPN endpoints to reduce false alerts. Specifically, administrators can modify the policy's sensitivity, include the organization's office IP addresses as trusted, and exclude known network ranges.
This approach directly aligns with the case study's scenario and satisfies the Defender for Cloud Apps requirement to reduce false positives while maintaining user anomaly detection accuracy.
Final Answer for Question 3: D. Impossible travel

NO.23 You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Log Analytics workspace to use: LA1
Windows 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 practices 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 level 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 (including 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 All 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.
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.

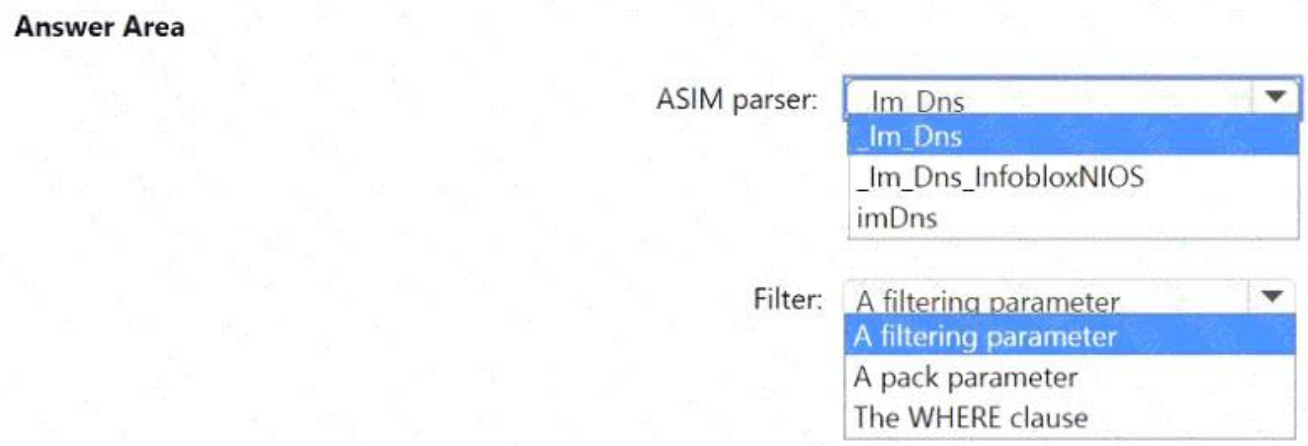
Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS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

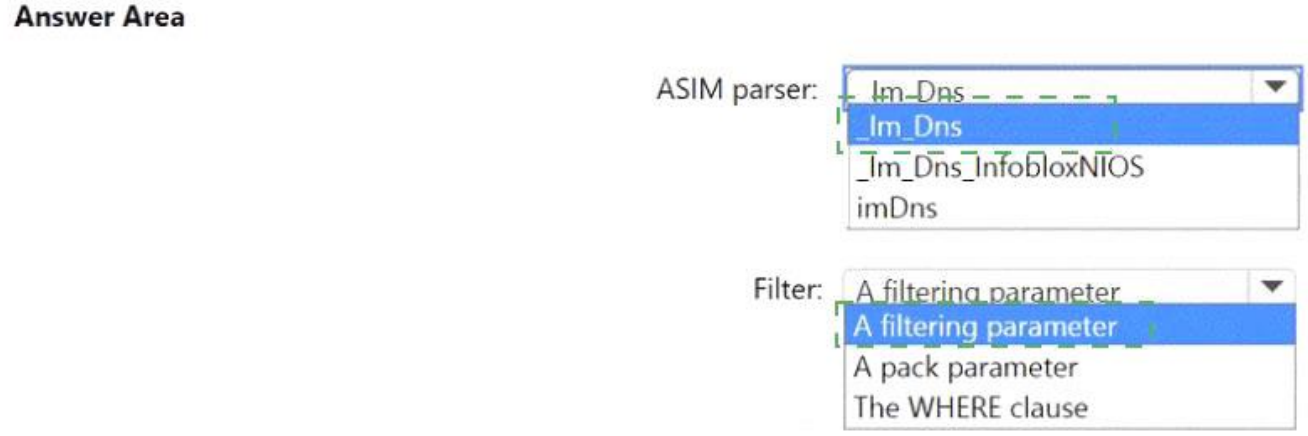
```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress,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

NO.24 You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Explanation:

In Microsoft Sentinel's Advanced Security Information Model (ASIM) , 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 recommended 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 NXDOMAIN responses for counting DNS request failures from Infoblox1 .

NO.25 You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

To monitor and detect higher-than-normal volumes of password resets, you need to gather password reset event data both from Azure Active Directory (cloud identities) and from on-premises Active Directory (domain accounts) . Microsoft's official Defender XDR and Sentinel integration guidance describes that:
* Azure AD Password Protection enforces and monitors password policies in both cloud and hybrid environments. It can detect weak, commonly used, or compromised passwords and logs related password change/reset activities. Deploying Azure AD Password Protection extends password reset visibility to on-premises domain controllers through the Password Protection proxy and DC agent. This makes it the correct choice for implementing monitoring at the identity environment level.
* In Microsoft Sentinel , to ingest and analyze password reset activities from on-premises servers (e.g., domain controllers), you must use the Windows Security Events via AMA connector . This connector collects Event ID 4723 (password change) , 4724 (password reset) , and related security logs directly from Windows Servers into the Sentinel Log Analytics workspace through the Azure Monitor Agent (AMA) . Once the events are available in Sentinel, they can be correlated with other identity or behavioral analytics to detect abnormal reset volumes or potential compromise attempts.
The other options are not suitable:

* Microsoft Defender for Identity focuses on identity compromise detection, not specifically on password reset volume monitoring.
* Smart lockout protects against brute-force sign-in attempts but doesn't generate detailed reset event telemetry.
* Microsoft security rule and UEBA are higher-level analytic configurations, not data ingestion mechanisms.
Therefore, to meet the Sentinel requirements for monitoring password reset anomalies:
Implement in the identity environment: Azure AD Password Protection
Configure in Microsoft Sentinel: The Windows Security Events via AMA connector

NO.26 You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?
A. Microsoft Sentinel Automation Contributor
B. Logic App Contributor
C. Automation Operator
D. Microsoft Sentinel Playbook Operator
Answer: A
Explanation:
The case study requires:
"Ensure that the Group1 members can create and edit playbooks."
In Microsoft Sentinel, the ability to create, edit, and assign playbooks is granted by the Microsoft Sentinel Automation Contributor role.
This role allows users to:
* Create and manage automation rules,
* Create and edit playbooks (Logic Apps) in the connected subscription,
* Associate playbooks with Sentinel incidents or alerts.
By contrast:
* Logic App Contributor allows Logic App creation but doesn't include Sentinel-level integration permissions.
* Automation Operator can run playbooks but not edit or create them.
* Sentinel Playbook Operator can execute playbooks but cannot modify or assign them.
# Answer for Question 11: A. Microsoft Sentinel Automation Contributor

NO.27 You need to implement the scheduled rule for incident generation based on rulequery1.
What should you configure first?
A. entity mapping
B. custom details
C. event grouping
D. alert details
Answer: C
Explanation:
The Sentinel requirement states:
"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." This behavior is controlled by the event grouping setting in the analytics rule configuration.

Microsoft Sentinel documentation explains:
"Event grouping determines how alerts generated from the same rule are grouped into incidents. Selecting
'Group all alerts triggered by this rule into a single incident' allows all related alerts to be combined."
Hence, configuring event grouping ensures that all alerts from rulequery1 related to the same user are consolidated into one incident, satisfying the requirement.
Answer for Question 10: C. event grouping

NO.28 You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account.
The solution must meet the Microsoft Sentinel requirements.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

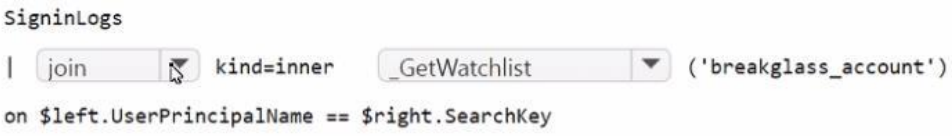
Answer Area

Answer:

Answer Area

Explanation:

Answer Area



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
_GetWatchlist(' < 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 requirement 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-minimizing 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 .

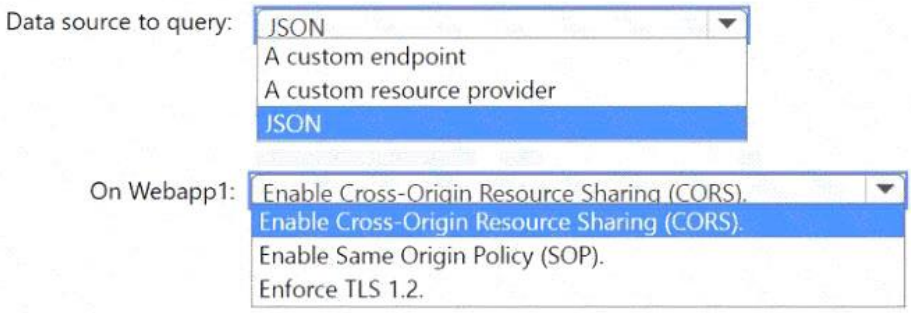
NO.29 You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?
A. a Microsoft Sentinel automation rule
B. a Microsoft Sentinel scheduled query rule
C. a Data Collection Rule (DCR)
D. an Azure Event Grid topic
Answer: C
Explanation:
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 scheduled 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.

NO.30 You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.
What should you create first?
A. a playbook with an incident trigger
B. a playbook with an entity trigger
C. an Azure Automation rule
D. a playbook with an alert trigger
Answer: A
Explanation:
Microsoft Sentinel playbooks can be triggered by different types of events- alerts , incidents , or

entities .
Since the requirement specifies "incidents generated by rulequery1" and asks for automatic processing of those incidents, the correct approach is to use a playbook with an incident trigger .
According to Microsoft Sentinel automation documentation:
"When you want automation to start after an incident is created or updated, use the incident trigger . This allows you to automate workflows such as closing incidents, adding comments, or sending notifications." This trigger type works with automation rules that specify when and how to execute playbooks based on incident state or severity. Using a playbook with an incident trigger meets the need for post-incident automation (e.g., auto-closing incidents if they match certain conditions).
Answer for Question 8: A. a playbook with an incident trigger

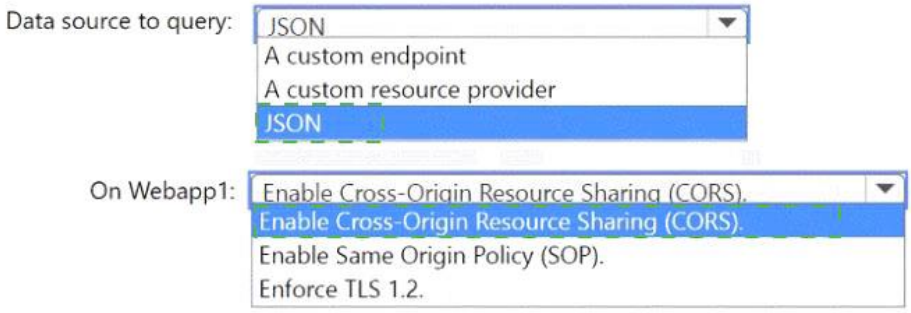
NO.31 You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



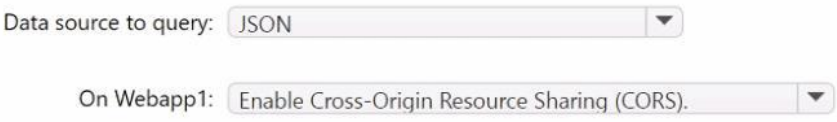
Answer:

Answer Area



Explanation:

Answer Area



To have a Microsoft Sentinel workbook pull live data from an external web service, you use the workbook's built-in JSON data source. Workbooks can query REST endpoints that return JSON and render results dynamically in visuals. Because the Azure portal (where the workbook runs) is a different origin than your on- prem/public Webapp1 , browsers will block these cross-origin requests unless the endpoint explicitly allows them. Therefore, the external service must enable CORS to permit the portal's origin to fetch the JSON. This aligns with Microsoft guidance that Workbooks can query HTTP/HTTPS JSON endpoints and that external endpoints must allow cross-origin requests for

client-side calls from the Azure portal. Enforcing CORS on Webapp1 satisfies the security model while enabling the workbook to retrieve data at view time-meeting the requirement to "dynamically retrieve data from Webapp1." Options like "custom endpoint" or "custom resource provider" aren't needed here, and enabling SOP or only enforcing TLS 1.2 wouldn't address the browser's cross-origin policy blocking the call.

NO.32 You need to implement the Defender for Cloud requirements.
What should you configure for Server2?

A. the Microsoft Antimalware extension

B. an Azure resource lock

C. an Azure resource tag

D. the Azure Automanage machine configuration extension for Windows

Answer: C

Explanation:
The requirement is to enable Microsoft Defender for Servers Plan 2 on all Azure VMs while excluding Server2 from agentless scanning . Defender for Cloud provides a built-in mechanism to exclude specific machines from agentless scanning based on resource tags . The process is: assign a distinct tag name:value to the VM you want to exclude (Server2), and then, in Defender for Cloud's Agentless scanning for machines settings, specify that tag pair under exclusions . Defender's continuous discovery honors these exclusions and skips any VM that matches the configured tag. This approach aligns with the business requirement of least privilege and minimal administrative effort : it avoids broad configuration changes, requires no extensions on the VM, and is reversible by simply removing or changing the tag. The Microsoft Antimalware extension and Automanage configuration are unrelated to agentless scanning behavior, and a resource lock would only prevent modifications/deletions, not scanning. Therefore, to meet the Defender for Cloud requirement precisely, configure an Azure resource tag on Server2 and reference that tag in the agentless scanning exclusion settings.

NO.33 You need to ensure that the configuration of HuntingQuery1 meets the Microsoft Sentinel requirements.
What should you do?

A. Add HuntingQuery1 to a livestream.

B. Create a watch list.

C. Create an Azure Automation rule.

D. Add HuntingQuery1 to favorites.

Answer: D

Explanation:
In Microsoft Sentinel, Hunting queries are used to proactively search for threats and anomalies across collected security data. The requirement states that HuntingQuery1 must run automatically when the Hunting page of Microsoft Sentinel is accessed. According to Microsoft's official Sentinel documentation, this behavior is achieved by adding the hunting query to "Favorites." When a query is marked as a favorite in the Sentinel Hunting blade, Sentinel automatically runs it every time the Hunting page is opened. This provides updated results without the need for manual execution, ensuring analysts always see the most current data for that query. This configuration also adheres to the organization's requirement to minimize administrative effort , since it eliminates the need for

scheduling, automation, or manual refresh actions.
Other options do not meet this functional requirement:
* A. Add to a livestream is used to monitor near-real-time data streams, not to auto-run queries upon accessing the Hunting page.
* B. Create a watchlist is used for referencing static external data sets (like IPs, users, or devices) inside KQL queries, not for automating hunting query execution.
* C. Create an automation rule applies to incident management workflows, not hunting query execution.
Therefore, as per Microsoft Sentinel's hunting documentation and best practices, the correct and verified answer is:
D). Add HuntingQuery1 to favorites .

NO.34 You need to implement the Defender for Cloud requirements.
Which subscription-level role should you assign to Group1?
A. Security Admin
B. Owner
C. Security Assessment Contributor
D. Contributor
Answer: C
Explanation:
The Defender for Cloud requirement states:
"The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives." According to Microsoft Defender for Cloud's RBAC documentation, the Security Assessment Contributor role provides permissions to:
* Enable and configure Defender plans,
* Manage security policies and initiatives,
* View and edit recommendations and compliance results.
This role gives enough permissions to perform Defender configuration tasks but follows the principle of least privilege , unlike broader roles like Owner or Contributor, which grant excessive rights.
Answer for Question 9: C. Security Assessment Contributor
Topic 4, Misc. Questions
Fabrikam. Inc. is a financial services company
The company has branch offices in New York. London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.
The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.
The fabrikam.com forest contains two global groups named Group1 and Group2.
All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license. Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.
Fabrikam has an Azure subscription that contains the resources shown in the following table.

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

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.
When the users use the VPN connections. Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives. Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.
Fabrikam plans to implement the following services:
* Microsoft Defender for Cloud
* Microsoft Sentinel
Fabrikam identifies the following business requirements:
* Use the principle of least privilege, whenever possible.
# Minimize administrative effort.
Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:
* Ensure that impossible travel alert policies are based on the previous activities of each user.
* Reduce the amount of impossible travel alerts that are false positives.
Minimize the administrative effort required to investigate the false positive alerts.
Fabrikam identifies the following Microsoft Defender for Cloud requirements:
* Ensure that the members of Group2 can modify security policies.
* Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
* Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
* Minimize the administrative effort required to investigate the false positive alerts.
Fabrikam identifies the following Microsoft Sentinel requirements:
* Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
* From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
* Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
* Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
* Ensure that App1 is available for use in Microsoft Sentinel automation rules.
* Identify the mean time to triage for incidents generated during the last 30 days.
* Identify the mean time to close incidents generated during the last 30 days.
* Ensure that the members of Group1 can create and run playbooks.
* Ensure that the members of Group1 can manage analytics rules.

* Run hunting queries on Pool! by using Jupyter notebooks.
* Ensure that the members of Group2 can manage incidents.
* Maximize the performance of data queries.
* Minimize the amount of collected data.

NO.35 You have an Azure subscription that contains a resource group named RG1. RG1 contains a Microsoft Sentinel workspace. The subscription is linked to a Microsoft Entra tenant that contains a user named User1.
You need to ensure that User1 can deploy and customize Microsoft Sentine1 workbook templates. The solution must follow the principle of least privilege.
Which role should you assign to User1 for RG1?

A. Workbook Contributor

B. Microsoft Sentinel Contributor

C. Contributor

D. Microsoft Sentinel Automation Contributor

Answer: A

Explanation:
To allow a user to deploy and customize Microsoft Sentinel workbook templates while maintaining the principle of least privilege, the correct role assignment is Workbook Contributor .
According to Microsoft Sentinel and Azure Monitor documentation, workbooks are stored as Azure resources under the resource group that hosts the Sentinel workspace. Microsoft specifies that: "Users who need to create, edit, or deploy workbooks require the Workbook Contributor role on the resource group that contains the workbooks. This role grants permissions to create and modify workbooks without allowing broader Sentinel or resource modifications." The Workbook Contributor role includes permissions such as Microsoft.Insights/workbooks/read , write , and delete , enabling full workbook editing capabilities. It does not grant access to analytics rules, incidents, or automation features, ensuring adherence to the least privilege principle.
By contrast:
* Microsoft Sentinel Contributor allows broader Sentinel configuration (analytics, playbooks, etc.), exceeding what's required.
* Contributor provides full access to manage all Azure resources, violating least privilege.
* Microsoft Sentinel Automation Contributor is intended for managing automation rules and playbooks, not workbooks.
Therefore, to enable User1 to deploy and customize Sentinel workbook templates in RG1 while maintaining minimal necessary permissions, assign Workbook Contributor on RG1 .