

Microsoft.SC-200.v2026-08-31.q179

Exam Code:	SC-200
Exam Name:	Microsoft Security Operations Analyst
Certification Provider:	Microsoft
Free Question Number:	179
Version:	v2026-08-31
# of views:	112
# of Questions views:	1972
https://www.freecram.net/torrent/Microsoft.SC-200.v2026-08-31.q179.html	

NEW QUESTION: 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a scheduled query rule for a data connector.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 2

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. All endpoint devices are onboarded to Microsoft Defender for Endpoint.

You have an Azure subscription that contains a Microsoft Sentinel workspace named Workspace 1. All Microsoft Defender XDR events are ingested into Workspace1.

You have a Microsoft Entra tenant.

You create a KQL query named query1 that searches device logs for a known vulnerability.

You need to ensure that query1 runs every hour. The solution must minimize administrative effort.

What should you configure?

A. an automation rule

B. automated investigation and response (AIR)

C. a watchlist

D. a custom detection rule

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 3

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. You need to implement deception rules. The solution must ensure that you can limit the scope of the rules.

What should you create first? A. device groups

- A. device groups
- B. device tags
- C. honeypot entity tags
- D. sensitive entity tags

Answer: ([SHOW ANSWER](#))

In Microsoft Defender XDR , deception rules (part of the Defender for Endpoint Deception capability) allow security teams to deploy decoys and honeypots to lure attackers. When configuring deception rules, scope management is essential to control which devices the rule applies to.

According to Microsoft's Defender XDR documentation:

"Deception rules can be targeted to specific devices or sets of devices by assigning them to device groups .

Device groups allow you to manage and scope rules, configurations, and alerts efficiently." Therefore, before creating a deception rule that must apply only to a specific subset of devices, you first create device groups - then assign the deception rule to those groups.

Final answer: A. device groups

NEW QUESTION: 4

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

- A. Deploy Azure Data Catalog to the West US Azure region.
- B. Modify the workspace settings of the existing Azure Sentinel deployment
- C. Add Microsoft Sentinel to a workspace.
- D. Create a data connector in Azure Sentinel.

Answer: ([SHOW ANSWER](#))

Azure Sentinel (now Microsoft Sentinel) is enabled per Log Analytics workspace . Each workspace operates independently; analytics rules in one Sentinel workspace cannot directly query another workspace's data unless Sentinel is also enabled there.

To use scheduled analytics rules against data in the LogsWest workspace, you must first add Microsoft Sentinel to that workspace . After Sentinel is enabled on LogsWest, you can create or connect analytics rules that query its data. You cannot simply modify workspace settings or connect data across regions without enabling Sentinel for the target workspace.

NEW QUESTION: 5

You have a Microsoft Sentinel workspace named Workspaces1.

The AzureActivity table in Workspace! has the following retention periods:

- * Interactive: 180 days
- * Total:180days

You need to modify the retention periods to meet the following requirements:

- * Minimize the costs associated with storing data in the table.
- * Maximize the period during which the table data remains available.

How should you configure each retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Interactive: 90 days

30 days

60 days

90 days

120 days

Total: 2 years

60 days

90 days

180 days

2 years

Microsoft

Answer:

Answer Area

Interactive: 90 days

30 days

60 days

90 days

120 days

Total: 2 years

60 days

90 days

180 days

2 years

Microsoft

Explanation:

Answer Area

Interactive: 90 days

Total: 2 years

Microsoft

In Microsoft Sentinel (Log Analytics), table retention uses two tiers: Interactive retention (hot, immediately queryable) and Archive (cold, queryable via Search/Restore). Sentinel includes up to 90 days of interactive retention at no additional cost ; extending interactive retention beyond 90 days incurs standard Log Analytics retention charges. To minimize cost , you should keep the interactive period at 90 days (the free tier).

For longer-term availability of data while still controlling costs, you set a higher Total retention so that, after the interactive window, data is moved to Archive storage at a significantly lower price per GB .

Archived data remains available to analysts using Search jobs or temporary Restore to hot for detailed queries.

Therefore, to maximize the period during which the table data remains available at the lowest cost, select the longest offered total retention, 2 years , which keeps older data in Archive instead of deleting it.

Thus, the optimal cost/availability configuration is Interactive = 90 days and Total = 2 years .

NEW QUESTION: 6

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.

```
| where TimeStamp > ago(2d)
| summarize activityCount = by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Answer:

```
| where TimeStamp > ago(2d)
| summarize activityCount = by FolderPath, FileName
ActionType, AccountDisplayName
| where activityCount > 5
```

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 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()

NEW QUESTION: 7

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

A. Create a records management disposition.

B. Perform a user data search.

C. Perform an audit search.

D. Perform a content search.

Answer: ([SHOW ANSWER](#))

In Microsoft Purview Compliance Portal, to locate specific email messages or files across user mailboxes and SharePoint/OneDrive content, you use Content Search (under eDiscovery or Content Search tools).

You can specify conditions such as Subject contains "Project1" and limit the search scope to specific users (those working on Project1).

* Records management disposition applies to retention policies.

* User data search is not a Purview feature.

* Audit search searches for user/admin activities, not message contents.

answer: D. Perform a content search

NEW QUESTION: 8

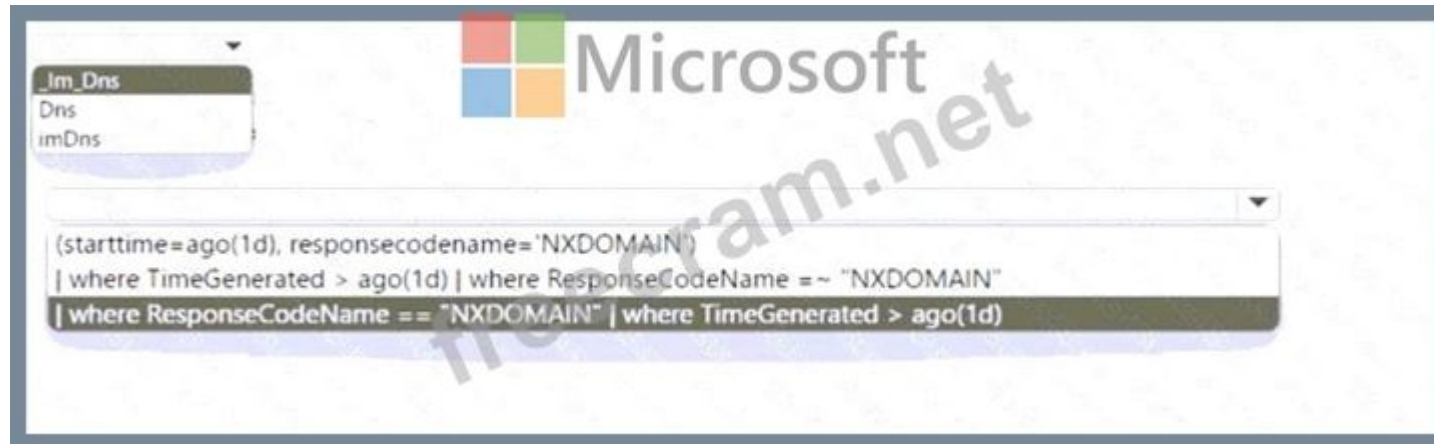
You have a Microsoft Sentinel workspace named Workspaces

You configure Workspace1 to c

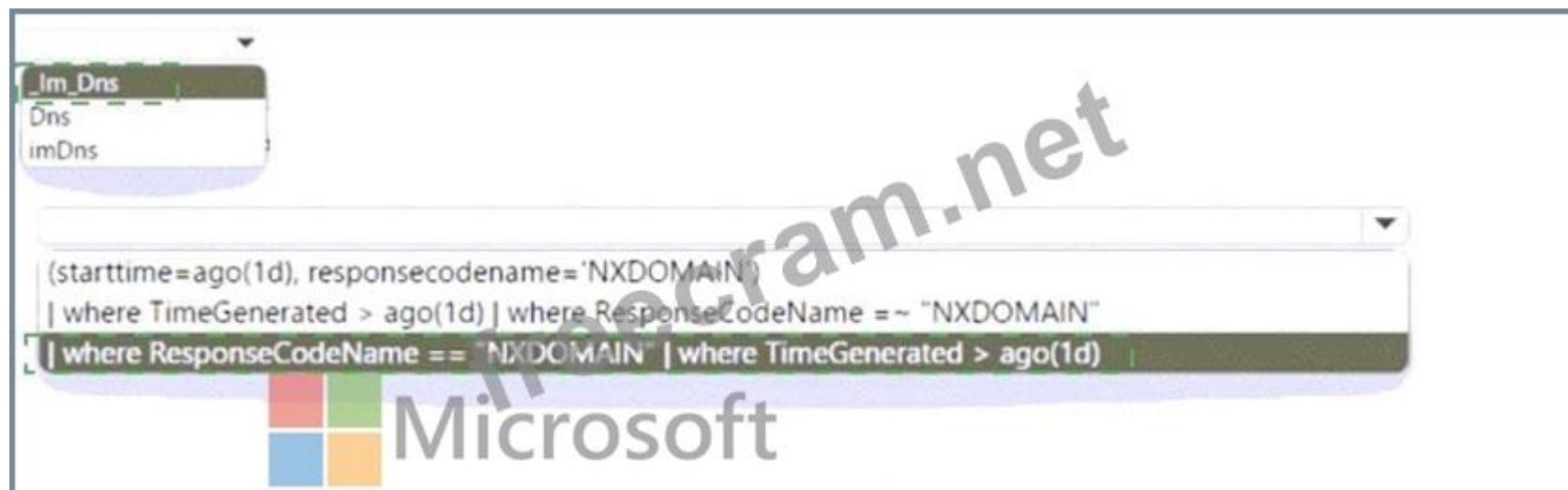
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of ' NXDOMAIN ' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.

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:



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, rather 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 to 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.

NEW QUESTION: 9

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server. You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the workspace created by Defender for Cloud, set the data collection level to Common
- B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.
- C. From the Azure portal, create an Azure Event Grid subscription.
- D. From the workspace created by Defender for Cloud, set the data collection level to All Events
- E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Answer: ([SHOW ANSWER](#))

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 involves 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 reducing 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 ensure 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

NEW QUESTION: 10

You have an on-premises Windows 11 Pro device named Device1 that is onboarded to Microsoft Defender for Endpoint You have a Microsoft 365 subscription.

You need to identify the processes running on Device1 and which network connections the processes have open. The solution must minimize administrative effort.

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

Actions

Run the netstat utility.

From the Action center, invoke an action.

Select View Map.

Initiate a live response session.

Navigate to the device page for Device1.

Collect an investigation package.

Extract the contents of the ZIP file.

Answer Area

Answer:

The screenshot shows the Microsoft Defender for Endpoint interface. On the left, under the 'Actions' tab, there is a list of actions: 'Run the netstat utility.', 'From the Action center, invoke an action.', 'Select View Map.', 'Initiate a live response session.', 'Navigate to the device page for Device1.', 'Collect an investigation package.', and 'Extract the contents of the ZIP file.'. On the right, under the 'Answer Area' tab, there is a list of actions: 'Initiate a live response session.', 'Navigate to the device page for Device1.', 'Collect an investigation package.', and 'Extract the contents of the ZIP file.'.

Explanation:

The screenshot shows the Microsoft Defender for Endpoint interface. On the left, under the 'Actions' tab, there is a list of actions: 'Run the netstat utility.', 'From the Action center, invoke an action.', and 'Select View Map.'. On the right, under the 'Answer Area' tab, there is a list of actions: '1 Initiate a live response session.', '2 Navigate to the device page for Device1.', '3 Collect an investigation package.', and '4 Extract the contents of the ZIP file.'.

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.

NEW QUESTION: 11

You have a Microsoft 365 subscription that uses Microsoft Copilot for Security.

You create a promptbook named Book1.

For Book1, you need to create a prompt that contains an input named IncidentID.

How should you format IncidentID?

- A. < IncidentID >
- B. \$IncidentID\$
- C. ##IncidentID##
- D. [IncidentID]

Answer: (SHOW ANSWER)

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 > .

NEW QUESTION: 12

You have a Microsoft Sentinel workspace.

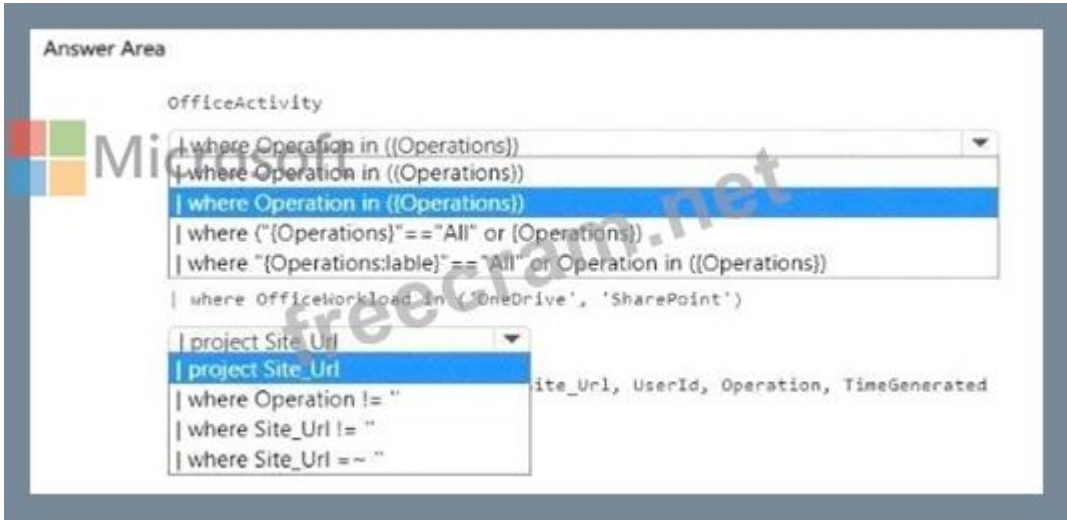
You plan to visualize data from Microsoft SharePoint Online and OneDrive sites.

You need to create a KQL query for the visual. The solution must meet the following requirements:

- * Select all workloads as a single operation.
- * Include two parameters named Operations and Users.
- * In the results, exclude empty values for the site URLs.

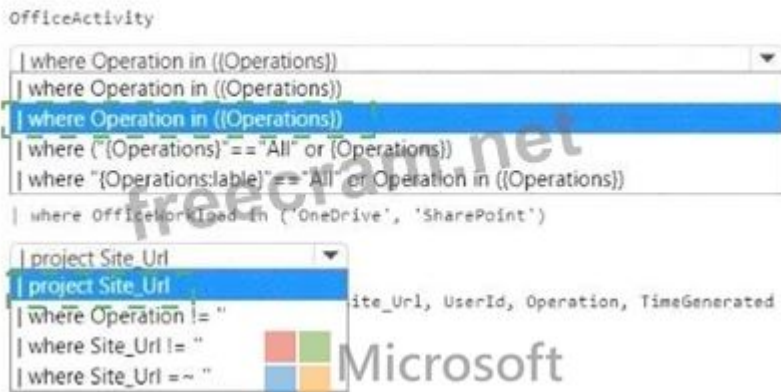
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE:

Each correct selection is worth one point.

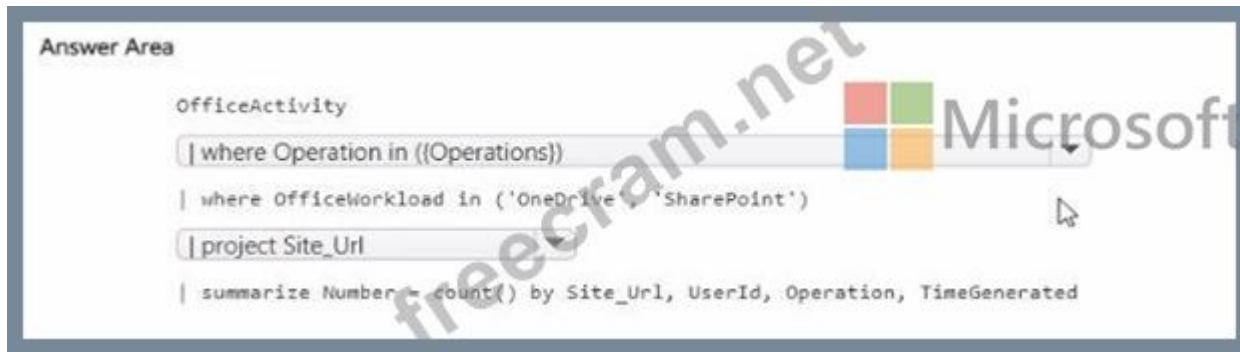


Answer:

Answer Area



Explanation:



In Microsoft Sentinel workbooks, parameters can be referenced directly in KQL. For multi-select parameters that include an All option, the recommended pattern is to check the parameter's label for "All" and otherwise filter by the selected values. Hence:

where (" {Operations:label} " == " All " or Operation in ({Operations})) This lets the visual treat All as a single choice while still supporting one or many explicit operations.

You also need a Users parameter, so you'd typically include:

| where UserId in ({Users})

Because the data source is OfficeActivity , to scope to SharePoint and OneDrive activity:

| where OfficeWorkload in (' OneDrive ' , ' SharePoint ')

Finally, to exclude empty site URLs , filter out blanks:

| where Site_Url != ''

Putting it together (for context):

OfficeActivity

| where (" {Operations:label} " == " All " or Operation in ({Operations}))

| where OfficeWorkload in (' OneDrive ' , ' SharePoint ')

| where UserId in ({Users})

| where Site_Url != ''

| project Site_Url, UserId, Operation, TimeGenerated

NEW QUESTION: 13

You have a Microsoft 365 E5 subscription that contains the hosts shown in the following table.

You have indicators in Microsoft Defender for Endpoint as shown in the following table.

D1 and ID2 reference the same tile as ID3

For each of the following statements, select Yes if the statement is true Otherwise, select No.

NOTE: Each correction selection is worth one point.

Statements	Yes	No
Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcb415dbe95f408b9ce91ee846ed.	☐	☐
Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	☐	☐
Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.	☐	☐

Answer:

Answer Area

Statements

Host1 will block the execution of a file that has the SHA-1 hash value of 2aae6c35c94fcb415dbe95f408b9ce91ee846ed.

Host2 will block and remediate a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.

Host3 will block the execution of a file that has the SHA-256 hash value of 88d4266fd4e6338d13b845fcf289579d209c897823b9217da3e161936f031589.

Yes

☐☐☐

No

☒☐☐

NEW QUESTION: 14

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert. What should you create first?

- A. a repository connection
- B. a watchlist
- C. an analytics rule
- D. an automation rule

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 15

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 16

You create a custom analytics rule to detect threats in Azure Sentinel.

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. The rule query takes too long to run and times out.
- B. The target workspace was deleted.
- C. Permissions to the data sources of the rule query were modified.
- D. There are connectivity issues between the data sources and Log Analytics

Answer: (SHOW ANSWER)

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.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

You have a Microsoft 365 subscription.

You plan to use Microsoft Defender XDR to hunt for email-related threats.

You need to identify sign-ins performed by users within 30 minutes of the users receiving a known malicious email.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft
freecram.net

```
MaliciousEmails=EmailEvents
Types has "Malware"
Email = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
(RecipientEmailAddress, "@")[0]); MaliciousEmails
logonEvents
= Timestamp, AccountName, DeviceName ) on AccountName
- TimeEmail) between (0min.. 30min)
```

Answer:

Answer Area

Microsoft
freecram.net

```
MaliciousEmails=EmailEvents
Types has "Malware"
Email = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
(RecipientEmailAddress, "@")[0]); MaliciousEmails
logonEvents
= Timestamp, AccountName, DeviceName ) on AccountName
- TimeEmail) between (0min.. 30min)
```

Explanation:

Microsoft
freecram.net

```
let MaliciousEmails=EmailEvents
| where ThreatTypes has "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(
split(RecipientEmailAddress, "@")[0]); MaliciousEmails
| join ( IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName ) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 30min)
```

NEW QUESTION: 18

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

- A. Microsoft Sentinel - Incidents
- B. Microsoft Sentinel - Workbooks
- C. Microsoft Sentinel
- D. Log Analytics workspaces

Answer: ([SHOW ANSWER](#))

To view incidents across multiple Sentinel workspaces (50 in this case), the central view is provided from the Microsoft Sentinel page in the Azure portal.

This page provides a multi-workspace incident view, allowing SOC analysts to see all incidents across all connected workspaces without switching manually.

* Microsoft Sentinel - Incidents # shows incidents from a single workspace only.

* Microsoft Sentinel - Workbooks # used for analytics visualization.

* Log Analytics workspaces # only for log storage and queries, not consolidated incident management.

Correct Answer: C. Microsoft Sentinel

NEW QUESTION: 19

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

- A. Playbooks
- B. Analytics
- C. Threat intelligence
- D. Incidents

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 20

The issue for which team can be resolved by using Microsoft Defender for Office 365?

- A. executive
- B. marketing
- C. security
- D. sales

Answer: ([SHOW ANSWER](#))

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 features 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.

NEW QUESTION: 21

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 22

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

- A. Yes
- B. No

Answer: ([SHOW ANSWER](#))

In Microsoft Defender for Identity, Honeytoken accounts are special decoy accounts designed to attract attackers. These accounts have no legitimate business use and are monitored closely-any authentication attempt or reconnaissance activity involving them triggers an alert.

Configuring such accounts is done through the Entity tags section in the Defender for Identity portal.

Microsoft documentation clearly states:

"Honeytoken accounts are decoy user accounts that Defender for Identity monitors for any authentication attempt. Configure them from the Entity tags settings." Thus, adding the accounts as Honeytoken accounts meets the goal perfectly - it allows monitoring and alerting when attackers attempt to exploit those accounts.

NEW QUESTION: 23

You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

* Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal

* Automatically associates the security principal with an Microsoft Sentinel entity 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

Microsoft

▼

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])
```

▼

AccountCustomEntity = Caller

| extend
| parse-where
| where

Answer:

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])

```

▼

AccountCustomEntity = Caller

extend

parse-where

where

Explanation:

AzureActivity Extend

Explanation = Use AzureActivity because NSG rule changes (operations like Microsoft.Network

/networkSecurityGroups/securityRules/write) are recorded 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 version 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.

NEW QUESTION: 24

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. You plan to create a Microsoft Defender XDR custom deception rule. You need to ensure that the rule will be applied to only 10 specific devices. What should you do first?

- A. Add the IP address of each device to the list of decoy accounts and hosts of the rule.
- B. Add the devices to a group.
- C. Add custom lures to the rule.
- D. Assign a tag to the devices

Answer: (SHOW ANSWER)

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).

NEW QUESTION: 25

You have an Azure subscription that uses Microsoft Sentinel.
You need to create a custom workbook that will calculate the average time it takes to close security incidents.
The solution must minimize administrative effort.
Which built-in Microsoft Sentinel workbook template should you select?

- A. Workspace Usage Report
- B. Incident Overview
- C. Investigation Insights
- D. Security operations efficiency

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 26

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You have a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.
Which three 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.

Actions

From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.

For the AD DS domain, configure Windows Event Forwarding.

For Sentinel1, configure the Windows Forwarded Events connector.

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

For Sentinel1, configure the Microsoft Defender for Identity connector.

For Sentinel1, enable UEBA.

Answer Area

Answer:

Actions

- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Answer Area

- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Explanation:

Actions

- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.

Answer Area

- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

To enable User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel and collect Active Directory Domain Services (AD DS) security events, the integration relies on Microsoft Defender for Identity (MDI)

. Defender for Identity monitors on-premises domain controllers and provides deep identity-based telemetry that Sentinel consumes for behavioral analytics and threat detection.

Here's the correct sequence explained step-by-step:

* Deploy Microsoft Defender for Identity on the AD DS domain

* Defender for Identity sensors must be installed on each domain controller (or dedicated server) in your on-premises AD DS environment.

* This step enables continuous monitoring of AD activities like logons, Kerberos authentications, and LDAP queries.

* Microsoft documentation states:

"To collect and analyze AD DS activities for UEBA, deploy Microsoft Defender for Identity sensors in your domain controllers."

* Configure the Microsoft Defender for Identity connector in Microsoft Sentinel

* In the Sentinel workspace (Sentinel1), go to Data connectors # Microsoft Defender for Identity # Connect .

* This connector ingests identity-related alerts and telemetry from Defender for Identity into Sentinel's Log Analytics workspace.

* It allows Sentinel to correlate identity-based security data with other sources for threat detection and investigation.

* Enable UEBA in Microsoft Sentinel

* After integrating MDI, enable UEBA in Sentinel's configuration settings.

* UEBA uses identity data (from MDI and Azure AD) and other logs to build behavioral baselines and detect anomalies such as lateral movement or privilege escalation.

* Microsoft documentation notes:

"To start analyzing user and entity behaviors, enable UEBA after connecting identity data sources such as Defender for Identity." Other actions listed (such as using legacy connectors or Windows Event Forwarding) are outdated or unnecessary when using MDI and Sentinel's built-in connectors.

NEW QUESTION: 27

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint and contains a user named user1 and a Microsoft 365 group named Group1. All users are assigned a Defender for Endpoint Plan 1 license.

You enable Microsoft Defender XDR Unified role-based access control (RBAC) for Endpoints & Vulnerability Management.

You need to ensure that User1 can configure alerts that will send email notifications to Group1. The solution must follow the principle of least privilege.

Which permissions should you assign to User1?

- A. Alerts investigation
- B. Manage security settings
- C. Defender Vulnerability Management - Remediation handling
- D. Live response capabilities: Basic

Answer: (SHOW ANSWER)

You have a Microsoft 365 subscription with Defender for Endpoint, and you've enabled Microsoft Defender XDR unified RBAC for Endpoints & Vulnerability Management. The requirement is that User1 should be able to configure alerts (i.e. set up rules that send email notifications) such that emails go to Group1, and you want to follow least privilege-that is, grant the minimal permission necessary for that capability.

Microsoft's official documentation states:

"Only users with 'Manage security settings' permissions can configure email notifications." Microsoft Learn Thus, in the Defender XDR RBAC model, the permission that allows a user to create or modify email notification alert rules is tied to Manage security settings (also referred to as core security settings in some documentation) .

Furthermore, the "Alert policies in the Microsoft Defender portal" article indicates that to create or edit alert policies (i.e. rules that govern how alerts behave and who they notify), you need the Manage Alerts role or equivalent permissions. However, in the unified RBAC model, managing alert policies overlaps with the broader "security settings" capability. Microsoft Learn Therefore:

* Granting Manage security settings gives exactly the ability required to configure email notification rules for alerts (including targeting the Microsoft 365 group) without giving broader investigative or remediation privileges.

* Other permissions-e.g., "Alerts investigation" (allows investigating alerts), "Defender Vulnerability Management - Remediation handling" (for handling remediation tasks), or "Live response capabilities: Basic" (for remote response actions)-do not cover alert notification configuration.

Hence the correct, least-privilege RBAC permission to assign to User1 is Manage security settings.

NEW QUESTION: 28

You need to implement Microsoft 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 Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

Query element required to correlate data between tenants:

Answer:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

Explanation:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

In Microsoft Sentinel, each workspace 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 to. 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, letting 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

NEW QUESTION: 29

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

The security team at your company detects command and control (C2) agent traffic on the network. Agents communicate once every 50 hours.

You need to create a Microsoft Defender XDR custom detection rule that will identify compromised devices and establish a pattern of communication. The solution must meet the following requirements:

* Identify all the devices that have communicated during the past 14 days.

* Minimize how long it takes to identify the devices.

To what should you set the detection frequency for the rule?

A. Every three hours

- B. Every 24 hours
- C. Every hour
- D. Every 12 hours

Answer: ([SHOW ANSWER](#))

When creating custom detection rules in Microsoft Defender XDR (formerly Microsoft 365 Defender) , the detection frequency determines how often the rule runs to evaluate the specified KQL query against the dataset.

In this scenario, the objective is to detect command and control (C2) agent traffic that communicates once every 50 hours (approximately every 2 days) , while still covering the past 14 days of device telemetry. The requirements emphasize:

- * Identifying all devices that have communicated in the past 14 days , and
- * Minimizing detection latency (how quickly compromised devices are identified), while balancing query efficiency and cost .

Analysis of Options

Option

Frequency

Evaluation

A). Every 3 hours

Too frequent for agents that beacon every ~50 hours. Creates unnecessary computation and no added detection benefit.

B). Every 24 hours

Optimal. Ensures daily evaluation, aligning with Defender XDR's typical log ingestion latency and well within the 50-hour communication window. Provides timely identification without resource waste.

C). Every hour

Excessively frequent; consumes unnecessary compute resources and does not improve detection effectiveness because C2 traffic occurs only once every 50 hours.

D). Every 12 hours

Slightly faster than daily but still redundant given the 50-hour beacon interval. Adds cost without significantly reducing time to detection.

Microsoft Official Guidance Microsoft's Defender XDR documentation states:

"For rules that identify infrequent or periodic activities, such as command-and-control communications or rare logon patterns, set the detection frequency based on the expected activity interval to minimize cost and optimize performance. For daily or multi-day behaviors, a frequency of 24 hours is recommended." Because the C2 agents communicate every 50 hours, a 24-hour detection frequency ensures the query executes often enough to detect compromised devices promptly while avoiding redundant runs or excess processing overhead.

Final Answer: B. Every 24 hours

NEW QUESTION: 30

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.

You need to identify all the changes made to sensitivity labels during the past seven days.

What should you use?

- A. the Incidents blade of the Microsoft 365 Defender portal
- B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
- C. Activity explorer in the Microsoft 365 compliance center
- D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: ([SHOW ANSWER](#))

Labeling activities are available in Activity explorer.

For example:

Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.

It is captured at the time of save in Office native applications and web applications.

It is captured at the time of occurrence in Azure Information protection add-ins.

Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide>

NEW QUESTION: 31

You have an Azure subscription.

You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

- * Minimize costs for daily ingested data.

- * Maximize the data retention period without incurring extra costs.

What should you do for each requirement? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.
Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

Answer:

Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.
Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

Explanation:

Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.
Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

When designing a Microsoft Sentinel workspace, cost optimization and data retention management are two key considerations. Microsoft Sentinel stores data in an Azure Log Analytics workspace , and pricing for data ingestion and retention is managed through Log Analytics settings.

* Minimize costs for daily ingested data: Microsoft's documentation on Log Analytics pricing models states that you can choose between Pay-As-You-Go (PAYG) and Commitment Tiers . The Commitment Tier model allows you to commit to a fixed amount of daily ingestion (for example, 20 GB/day in this case) at a lower per-GB cost compared to PAYG pricing. If your ingestion volume is predictable (as in this scenario-20 GB per day), this model provides significant cost savings without the administrative overhead of managing caps or throttling. Therefore, to minimize ingestion cost, the correct choice is "Use a commitment tier."

* Maximize the data retention period without incurring extra costs: By default, Microsoft Sentinel (via Log Analytics) provides 90 days of data retention at no additional charge . Extending retention beyond 90 days incurs additional storage charges. According to Microsoft's official guidance, "Log Analytics retains data for 90 days at no cost; data kept beyond that period is billed at the retention rate." Therefore, to maximize the free retention period while avoiding extra cost, the correct configuration is "Set retention to 90 days."

Summary:

* Minimize costs for daily ingested data # Use a commitment tier

* Maximize retention without extra costs # Set retention to 90 days

This configuration ensures both cost efficiency and maximum free data availability, aligning with Microsoft Security Operations (SecOps) and Sentinel best practices.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

You have a Microsoft Sentinel workspace named Workspace1.

You need to run a KQL query as a search job.

Which five actions should you perform in Workspace 1 in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Select Logs.

Enter a KQL query and select Run.

Select Search.

Set Search job mode to On.

Enter a KQL query and select Search job.

Enter a new table name.

Select Run a search job.

Answer Area

Answer:

Actions

⋮ Select Logs.
⋮ Enter a KQL query and select Run.
⋮ Select Search.
⋮ Set Search job mode to On.
⋮ Enter a KQL query and select Search job.
⋮ Enter a new table name.
⋮ Select Run a search job.

Answer Area

⋮ Select Search.
⋮ Set Search job mode to On.
⋮ Enter a KQL query and select Search job.
⋮ Enter a new table name.
⋮ Select Run a search job.

Explanation:

Actions

⋮ Select Logs.
⋮ Enter a KQL query and select Run.

Answer Area

1	⋮ Select Search.
2	⋮ Set Search job mode to On.
3	⋮ Enter a KQL query and select Search job.
4	⋮ Enter a new table name.
5	⋮ Select Run a search job.

NEW QUESTION: 33

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States- based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses.

You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.

You need to prevent alerts for legitimate sign-ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Override automatic data enrichment.

B. Add the IP addresses to the corporate address range category.

- C. Increase the sensitivity level of the impossible travel anomaly detection policy.
- D. Add the IP addresses to the other address range category and add a tag.
- E. Create an activity policy that has an exclusion for the IP addresses.

Answer: (SHOW ANSWER)

In Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security), the impossible travel and sign-in from risky IP addresses anomaly detection policies automatically analyze user activity patterns and compare sign-in locations to detect suspicious behavior. However, when legitimate corporate IPs are not correctly identified as trusted, these policies may generate excessive false positives. According to Microsoft's official documentation on managing IP address ranges:

"To reduce false positive alerts from trusted network locations, define your organization's known IP address ranges in the Defender for Cloud Apps portal. Tagging these as Corporate ensures that sign-ins originating from these IPs are treated as safe and excluded from anomaly detection alerts." To implement this properly:

- * Add the IP addresses to the Corporate address range category (Option B) - This explicitly identifies these ranges as trusted corporate networks. Once defined, Microsoft Cloud App Security (MCAS) automatically suppresses anomaly alerts (like impossible travel or risky IP alerts) from these known sources.
- * Override automatic data enrichment (Option A) - Automatic data enrichment uses Microsoft's threat intelligence and geolocation services to classify IPs. When you override it, the system respects your manual classification (Corporate, VPN, Risky, etc.) rather than reclassifying based on Microsoft's enrichment data. This ensures that your defined corporate IPs remain categorized correctly, avoiding repeated alerting on known legitimate sign-ins.

The other options are not appropriate:

- * C. Increase sensitivity level would actually make alerts even more frequent rather than reduce them.
- * D. Add IPs to "other" category does not stop alerts; only the Corporate category suppresses impossible travel alerts.
- * E. Activity policy exclusion is not used for anomaly detection tuning; it applies to specific custom activity conditions.

Therefore, the correct configuration to suppress legitimate corporate alerts and follow best practice for false positive reduction is to override automatic data enrichment (A) and add corporate IPs to the Corporate address range category (B).

NEW QUESTION: 34

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Answer: (SHOW ANSWER)

In Microsoft Defender for Endpoint (part of Microsoft Defender XDR), device groups are used to organize endpoints for policy, automation, and investigation purposes. Tags provide a dynamic way to categorize devices temporarily or permanently.

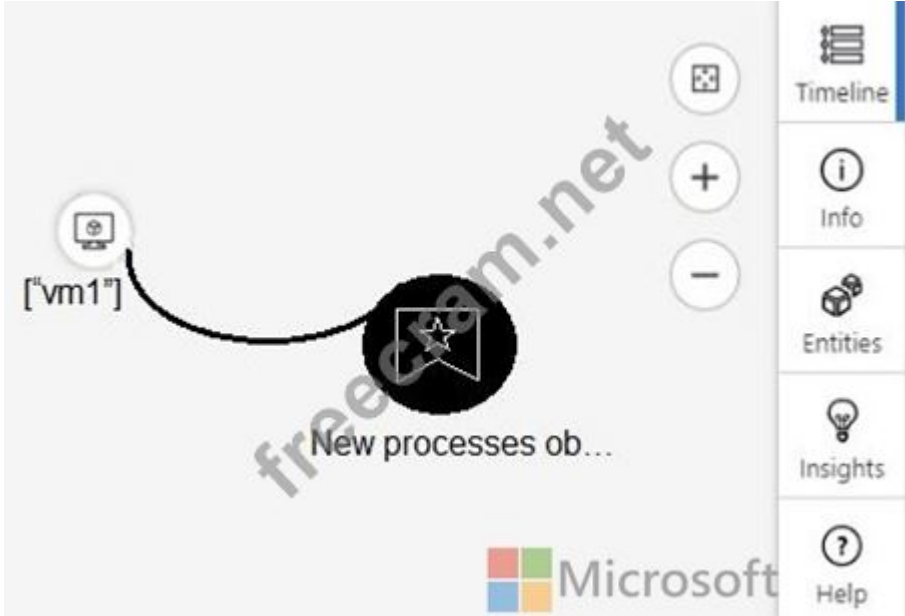
To temporarily group high-value machines for investigation or response, the correct approach is to use tags and a new high-rank device group :

- * Add a tag to the machines (C): Applying a tag allows quick identification and dynamic inclusion in a new group without permanently altering membership.
- * Create a new device group (D): Creating a device group with a rank of 1 ensures it has the highest precedence and that devices tagged for this group are included immediately.
- * Add a tag to the device group (A): The device group's membership rule can include the tag value, automating group inclusion.

This approach aligns with Microsoft Defender for Endpoint guidance to "use device tags and group ranks for dynamic grouping and prioritized policy application" - minimizing administrative effort while allowing targeted response actions.

NEW QUESTION: 35

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.

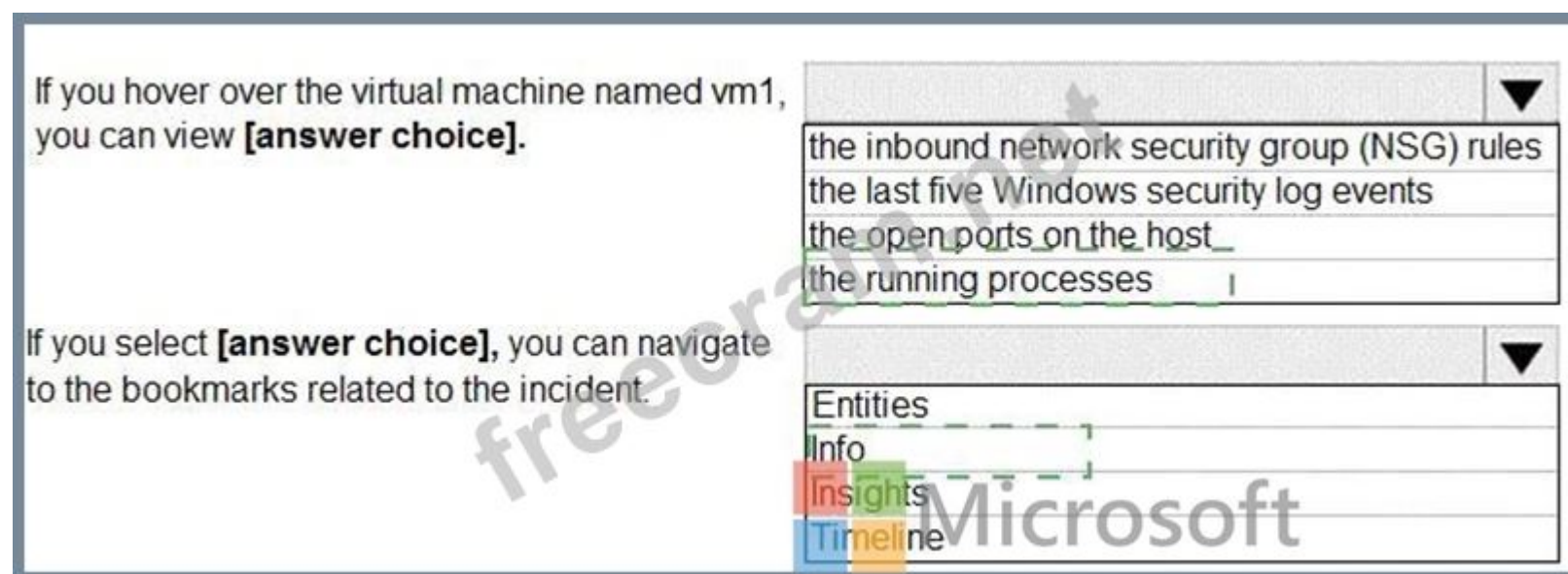


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If you hover over the virtual machine named vm1, you can view [answer choice].	▼ the inbound network security group (NSG) rules the last five Windows security log events the open ports on the host the running processes
If you select [answer choice], you can navigate to the bookmarks related to the incident.	▼ Entities Info Insights Timeline

Answer:



Explanation:

If you hover over the virtual machine named vm1 , you can view the running processes .

If you select Info , you can navigate to the bookmarks related to the incident.

NEW QUESTION: 36

You have a Microsoft 365 E5 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

All Windows devices are on boarded to Microsoft Defender for Endpoint.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third- party antivirus product.

Solution: You enable Live Response.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

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 artifacts 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 remediate undetected malicious artifacts at scale. Therefore enabling Live Response alone does not meet the stated protection goal.

NEW QUESTION: 37

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 38

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall.

C. Create an application security group.

D. Modify the access policy for the key vault.

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 39

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Answer: ([SHOW ANSWER](#))

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 .

NEW QUESTION: 40

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

- A. Security solutions
- B. Security policy
- C. Pricing & settings
- D. Security alerts
- E. Azure Defender

Answer: ([SHOW ANSWER](#))

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 .

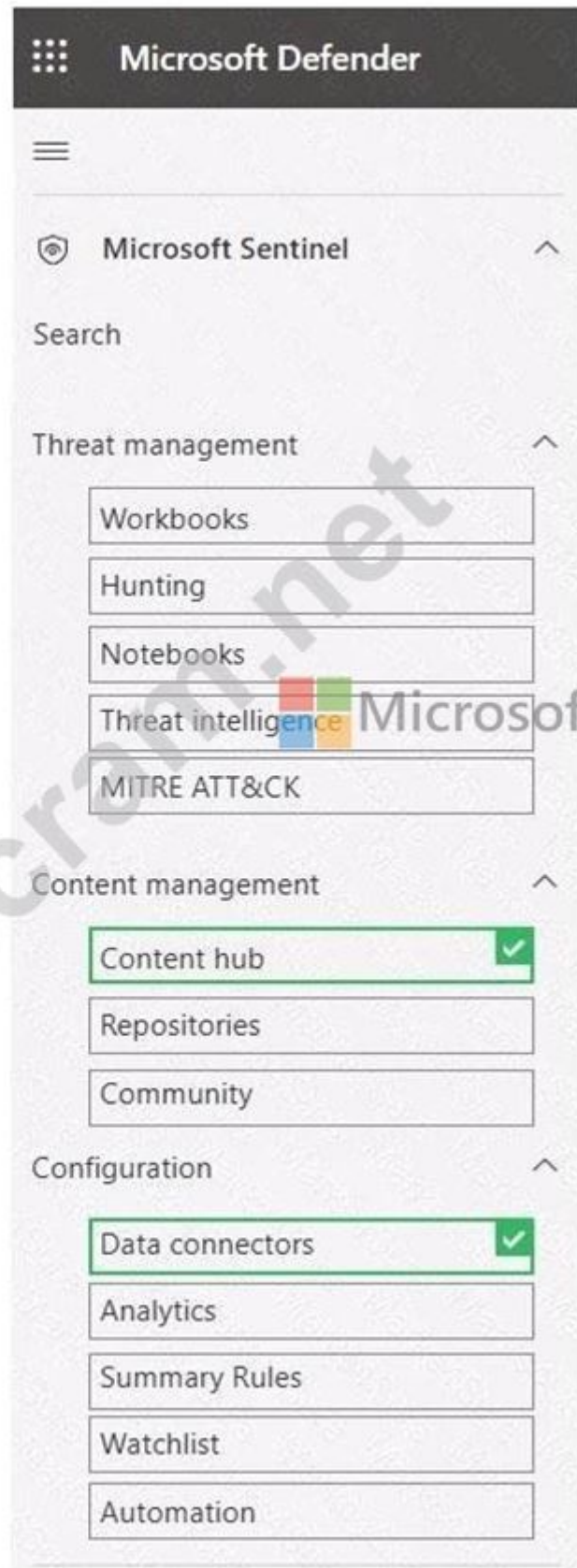
NEW QUESTION: 41

You have a Microsoft 365 E5 subscription.

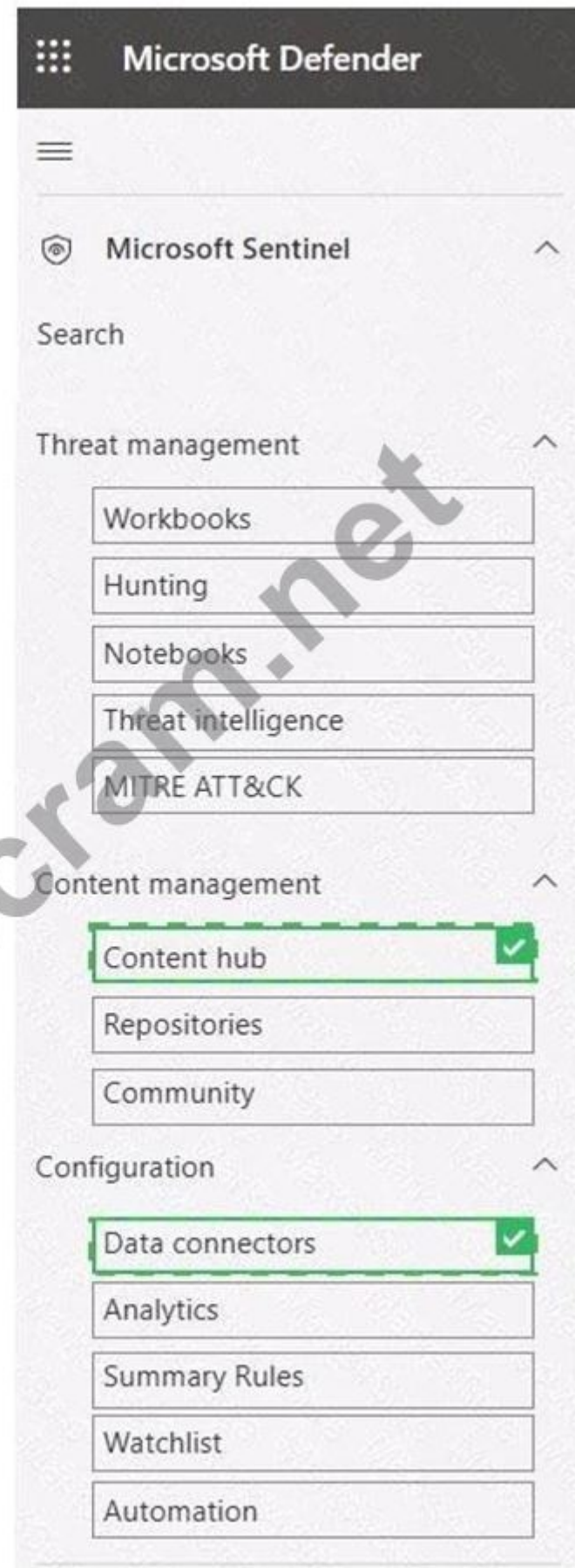
You need to configure Microsoft Sentinel to collect logs from Microsoft Entra.

Which two nodes should you use in the Microsoft Defender portal? To answer, select the appropriate nodes in the answer area.

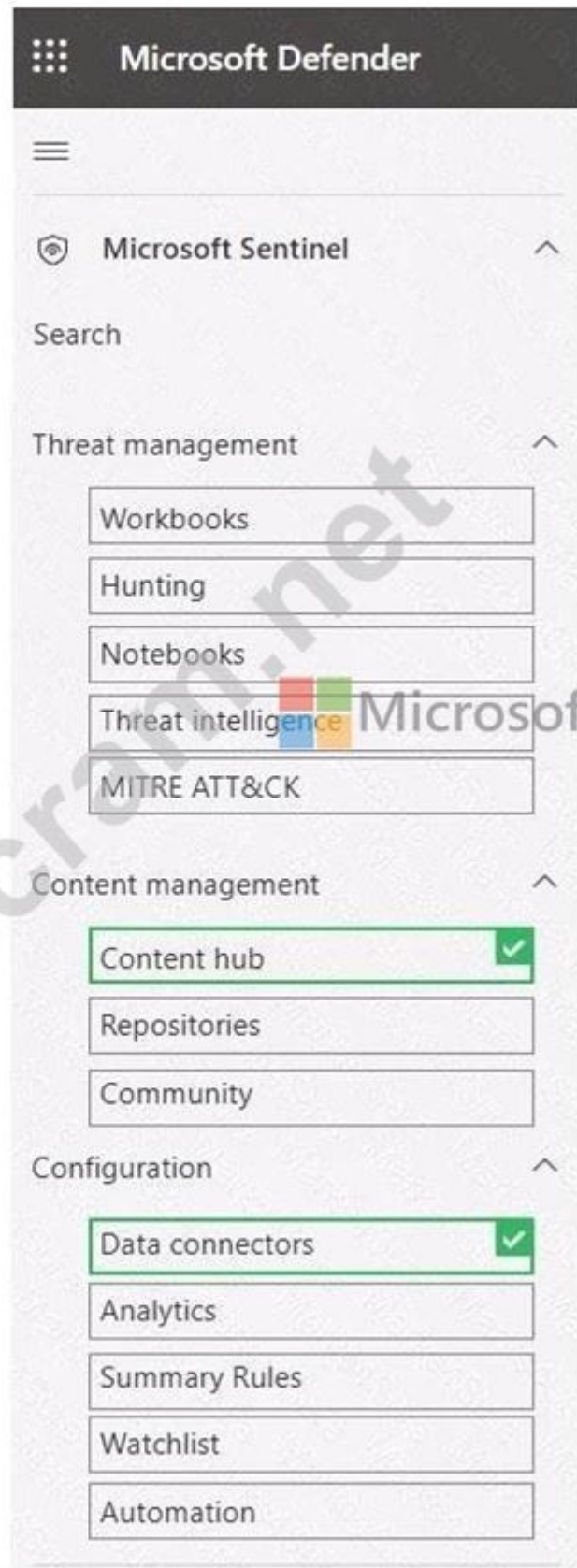
NOTE: Each correct answer is worth one point.



Answer:



Explanation:



NEW QUESTION: 42

You have a Microsoft 365 E5 subscription that contains 500 Windows 11 devices.
 You have a Microsoft Defender for Endpoint deployment that has the following settings:
 * Discovery mode: Basic

- * Live Response: Disabled
- * Enable EDR in block mode: Off
- * Tamper Protection: Off

You need to implement automatic attack disruption in Microsoft Defender XDR.

What should you do?

- A.** Set Enable EDR in block mode to On.
- B.** Set Live Response to On.
- C.** Change Discovery mode to Standard discovery.
- D.** Set Tamper Protection to On.

Answer: ([SHOW ANSWER](#))

Microsoft Defender XDR's Automatic attack disruption requires EDR in block mode to be enabled. This feature allows Defender for Endpoint to block or contain malicious activities, even when the primary antivirus engine fails to detect or block them initially.

According to Microsoft Defender documentation, attack disruption relies on real-time EDR response capabilities and EDR in block mode to isolate compromised users or devices automatically. Without EDR in block mode, Defender can only alert - not stop - ongoing attacks.

Enabling EDR in block mode integrates the EDR layer with Microsoft Defender Antivirus to automatically contain lateral movement and credential theft activities. While Tamper Protection, Live Response, and Standard Discovery are valuable, they do not directly enable automatic attack disruption.

Correct answer: A. Set Enable EDR in block mode to On

NEW QUESTION: 43

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a custom report that will visualise sign-in information over time.

What should you create first?

- A.** a workbook
- B.** a hunting query
- C.** a notebook
- D.** a playbook

Answer: ([SHOW ANSWER](#))

A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription. Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview>

NEW QUESTION: 44

You have an on-premises datacenter that contains a custom web app named Appl. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You receive an alert that a user downloaded highly confidential documents.

You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

For App1 to require MFA, use:

To implement a session policy, use:

Answer:

Answer Area

For App1 to require MFA, use:

To implement a session policy, use:

Explanation:

Answer Area

For App1 to require MFA, use:

To implement a session policy, use:

In this scenario, App1 is a custom web app published through Microsoft Entra Application Proxy and authenticated using Active Directory Domain Services (AD DS) . Because it's integrated with Microsoft Entra ID (formerly Azure AD) for access control, the most appropriate and supported way to require MFA for users accessing the application is through Conditional Access .

Microsoft Entra Conditional Access policies evaluate user sign-in conditions such as risk level, device compliance, location, and sensitivity of data before granting access. Specifically, Microsoft's documentation states:

"Conditional Access policies allow administrators to require multi-factor authentication, block access, or enforce specific controls such as app protection or session policies for cloud and on-premises applications integrated with Microsoft Entra ID." Therefore, to make MFA mandatory for users accessing App1, a Conditional Access policy must be created targeting that application.

For the second part, to implement a session policy that controls or monitors user behavior (such as downloading highly confidential documents), the correct choice is Microsoft Defender for Cloud Apps (MDA) . Microsoft's official guidance says:

"Session policies in Microsoft Defender for Cloud Apps provide real-time session controls that enable administrators to monitor and restrict user activity in cloud apps, including download, cut/copy, and upload actions based on sensitivity labels or user risk." These session policies integrate seamlessly with Conditional Access via the "Use Conditional Access App Control" setting to apply continuous access evaluation during a user's session.

Hence, the correct verified configuration is:

- * Require MFA: Conditional Access
- * Implement session policy: Microsoft Defender for Cloud Apps

NEW QUESTION: 45

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.

You need to mitigate the following device threats:

- * Microsoft Excel macros that download scripts from untrusted websites
- * Users that open executable attachments in Microsoft Outlook
- * Outlook rules and forms exploits

What should you use?

- A.** Microsoft Defender Antivirus
- B.** attack surface reduction rules in Microsoft Defender for Endpoint
- C.** Windows Defender Firewall
- D.** adaptive application control in Azure Defender

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 46

You have 500 on-premises Windows 11 devices that use Microsoft Defender for Endpoint You enable Network device discovery.

You need to create a hunting query that will identify discovered network devices and return the identity of the onboarded device that discovered each network device.

Which built-in function should you use?

- A.** current_cluster,endpoint()
- B.** DeviceFromIP ()
- C.** next ()
- D.** SeenBy ()

Answer: ([SHOW ANSWER](#))

In Microsoft Defender for Endpoint advanced hunting, when Network device discovery is enabled, onboarded devices can detect other devices on the same network. To build a hunting query that identifies discovered network devices and shows which onboarded device discovered each, you use the SeenBy() built-in function.

Microsoft's official Defender XDR KQL function documentation explains:

"The SeenBy() function returns the list of devices that have observed the entity (for example, IP address, URL, or network device). This function is typically used to correlate discovered devices with the onboarded devices that detected them." For example, you can write:

```
DeviceNetworkInfo
```

```
| where NetworkDeviceRole == " Discovered "
```

| extend DiscoveringDevice = SeenBy()

This function effectively maps the discovered asset to the detecting (onboarded) device.

Other options are not applicable:

* current_cluster,endpoint() - not a valid Defender hunting function.

* DeviceFromIP() - resolves IP addresses to onboarded devices but does not show which device discovered another.

* next() - a general KQL operator for sequencing data, not for correlating network discovery events.

Therefore, to identify discovered network devices and the discovering endpoints, the correct built-in function is SeenBy() .

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

You have a Microsoft Sentinel workspace that has a default data retention period of 30 days. The workspace contains two custom tables as shown in the following table.

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

Each table ingested two records per day during the past 365 days.

You build KQL statements for use in analytic rules as shown in the following table.

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)

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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 .	☐	☐

Answer:

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 .	☒	☐

NEW QUESTION: 48

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra role: Global Administrator

Role for WS1: Microsoft Sentinel Contributor

Answer:

Answer Area

Microsoft Entra role: Global Administrator

Role for WS1: Contributor

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

NEW QUESTION: 49

You have a custom Microsoft Sentinel workbook named Workbooks.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

A. In the query editor interface, configure Settings.

B. In the query editor interface, select Advanced Editor

C. In the grid query, include the project operator.

D. In the grid query, include the take operator.

Answer: ([SHOW ANSWER](#))

In Microsoft Sentinel workbooks , when displaying query results in a grid visualization , you can limit the number of displayed rows by using KQL query operators. The take operator in Kusto Query Language (KQL) is specifically designed to restrict output to a fixed number of records.

Microsoft Sentinel workbook guidance states:

"To control the number of results returned in a workbook grid, use the KQL take operator. For example, adding | take 100 ensures that only 100 rows are returned and displayed." This approach enforces both performance efficiency and readability, ensuring large result sets don't overload the visualization.

Other options are incorrect:

- * Settings and Advanced Editor adjust workbook configuration, not query limits.

- * Project only selects specific columns, not row count.

Correct answer: D. In the grid query, include the take operator

NEW QUESTION: 50

You have a Microsoft Sentinel workspace named SW1.

You need to identify which anomaly rules are enabled in SW1.

What should you review in Microsoft Sentinel?

A. Settings

B. Entity behavior

C. Analytics

D. Content hub

Answer: **C** ([LEAVE A REPLY](#))

To identify which anomaly rules are enabled in a Microsoft Sentinel 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 (specifically under the Anomalies tab).

NEW QUESTION: 51

You have a Microsoft 365 subscription that uses Microsoft Security Copilot. You have the files shown in the following table.

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

Each file contains a copy of your company ' s compliance policy.

You need to ensure that Security Copilot responses are informed by the compliance policy. Which files can be uploaded to Security Copilot?

- A.** File1.docx and File3.txt only
- B.** File3.txt only
- C.** File1.docx only
- D.** File1.docx, File2.pdf, and File3.txt
- E.** File2.pdf and File3.txt only

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

- A.** In workspace1, install a solution.
- B.** In sub1, register a provider.
- C.** From Security Center, create a Workflow automation.
- D.** In workspace1, create a workbook.

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 53

You have a Microsoft Sentinel workspace that contains a custom workbook named Workbook1.

You need to create a visual in Workbook1 that will display the logon count for accounts that have logon event IDs of 4624 and 4634.

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

NOTE Each correct selection is worth one point.

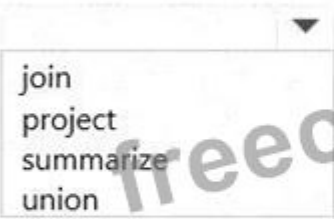
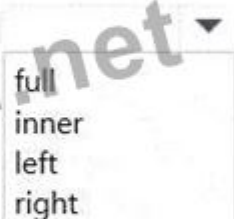
Answer Area

SecurityEvent

| where EventID == "4624"

| summarize LogOnCount=count() by EventID, Account

| project LogOnCount, Account

|  kind =  (

SecurityEvent

| where EventID == "4634"

| summarize LogOffCount=count() by EventID, Account

| project LogOffCount, Account

 Microsoft
) on Account

Answer:

Answer Area

SecurityEvent

| where EventID == "4624"

| summarize LogOnCount=count() by EventID, Account

| project LogOnCount, Account

|  kind = (

SecurityEvent

| where EventID == "4634"

| summarize LogOffCount=count() by EventID, Account

| project LogOffCount, Account

) on Account

Explanation:

First dropdown: join

Second dropdown: full

In Microsoft Sentinel and Kusto Query Language (KQL), when you need to combine two tables based on a common field, you use the join operator. In this scenario, both queries pull from the same SecurityEvent table but filter on different Event IDs - 4624 for logon and 4634 for logoff events. To correlate or compare the two results by Account, you need to join them.

The first query returns the number of logon events per account (LogOnCount), while the second returns the number of logoff events per account (LogOffCount). The join key is Account, which exists in both result sets.

To ensure that all accounts - those who may have only logon events or only logoff events - are included in the visualization, you use a full join. A full join combines matching records from both sides and keeps unmatched records from either side, filling missing values with nulls. This ensures that every account with either a logon or a logoff count appears in the results.

Therefore, the correct query completion is:

SecurityEvent

| where EventID == " 4624 "

| summarize LogOnC ount = count() by EventID, Account

| project LogOnCount, Account

| join kind = full (

SecurityEvent

| where EventID == " 4634 "

| summarize LogOffCount = count() by EventID, Account

| project LogOffCount, Account
) on Account

This query gives a complete view of all accounts and their corresponding logon/logoff counts.

Correct selections:

* First box # join

* Second box # full

NEW QUESTION: 54

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

A. Incidents

B. Investigations

C. Advanced hunting

D. Remediation

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 55

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create a custom rule based on the Office 365 connector templates.

B. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.

C. Create a Microsoft Cloud App Security connector.

D. Create an Azure AD Identity Protection connector.

Answer: ([SHOW ANSWER](#))

To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:

* Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.

* Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules>

NEW QUESTION: 56

You have an Azure subscription named Sub1 that is linked to a Microsoft Entra tenant named contoso.com.

Contoso.com contains a user named User1. Sub1 contains a Microsoft Sentinel workspace.

You provision a Microsoft Copilot for Security capacity.

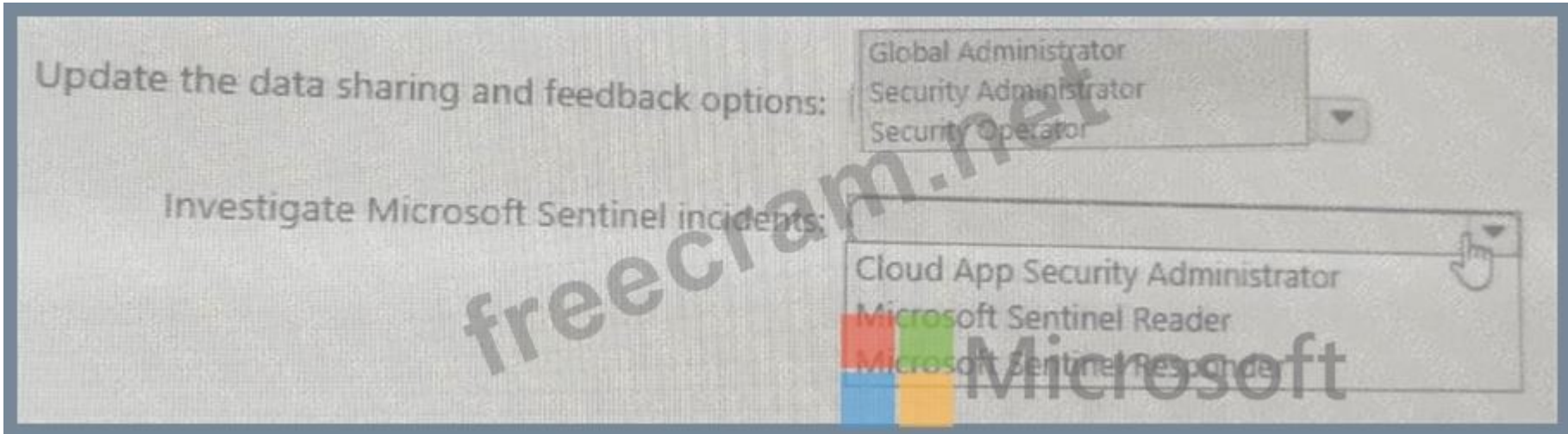
You need to ensure that User1 can use Copilot for Security to perform the following tasks:

- . Update the data sharing and feedback options.
- . Investigate Microsoft Sentinel incidents.

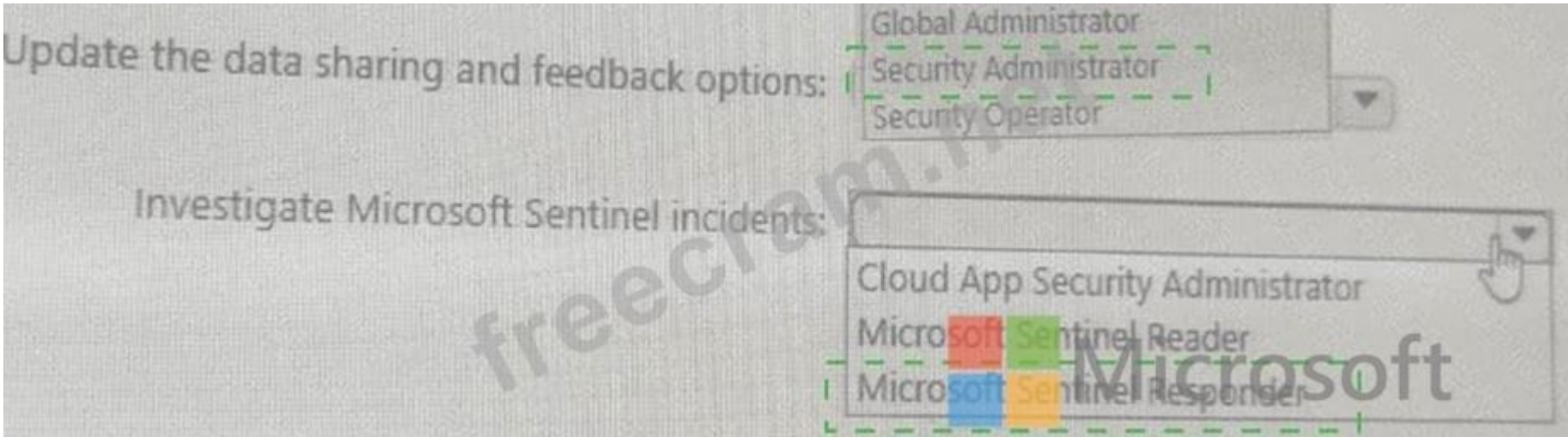
The solution must follow the principle of least privilege.

Which role should you assign to User1 for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point



Answer:



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 Cloud 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 control (RBAC) documentation.

NEW QUESTION: 57

You have an Azure subscription that contains a Log Analytics workspace.

You need to enable just-in-time (JIT) VM access and network detections for Azure resources.

Where should you enable Azure Defender?

A. at the subscription level

B. at the workspace level

C. at the resource level

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 58

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: (SHOW ANSWER)

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

NEW QUESTION: 59

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure Microsoft Defender for Endpoint:	Turn on endpoint detection and response (EDR) in block mode Turn on Live Response Turn off Tamper Protection
To configure the devices:	Add a network assessment job Create a device group that contains the devices and set Automation level to Full Create a device group that contains the devices and set Automation level to No automated response

Answer:

To configure Microsoft Defender for Endpoint:	Turn on endpoint detection and response (EDR) in block mode Turn on Live Response Turn off Tamper Protection
To configure the devices:	Add a network assessment job Create a device group that contains the devices and set Automation level to Full Create a device group that contains the devices and set Automation level to No automated response

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:

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

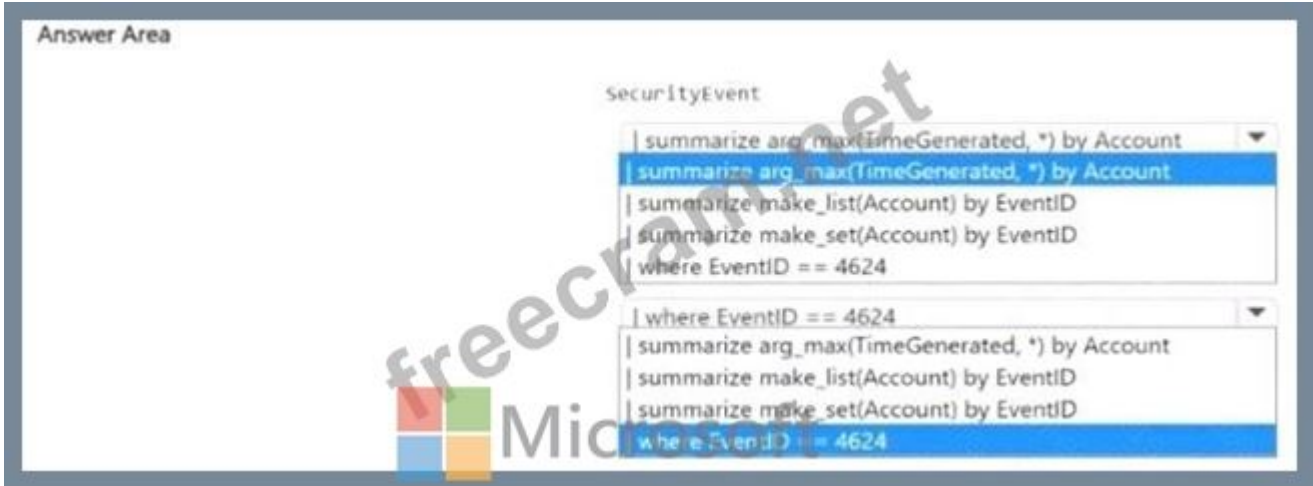
[view=o365-worldwide](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide)

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

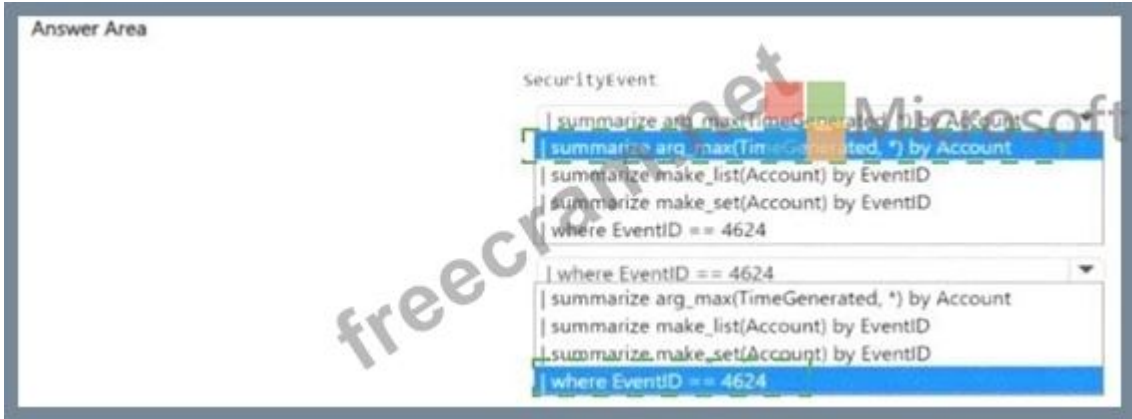
NEW QUESTION: 60

You need to build a KQL query in a Microsoft Sentinel workspace. The query must return the SecurityEvent record for accounts that have the last record with an EventID value of 4624. How should you complete the query ' To answer, select the appropriate options in the answer area.

NOTE: Each coned selection is worth one point



Answer:



Explanation:



SecurityEvent

| where EventID == 4624

| summarize arg_max(TimeGenerated, *) by Account

Comprehensive and Detailed Explanation with all Microsoft Security Operations (SecOps) documents: = This query is designed for Microsoft Sentinel (Log Analytics) to identify the latest successful logon (Event ID

4624) for each account. Event ID 4624 in the SecurityEvent table indicates a successful logon in Windows security logs.

Let's break down the logic step-by-step:

| where EventID == 4624

This line filters the SecurityEvent table to include only records that correspond to successful logon events.

Filtering first ensures that only relevant events are processed by the summarization step, improving performance and accuracy.

| summarize arg_max(TimeGenerated, *) by Account

The arg_max() aggregation function retrieves the record that has the maximum value of TimeGenerated for each Account.

The * symbol ensures that all columns from that most recent record are returned (not just TimeGenerated and Account).

In this context, this means we get the most recent 4624 logon event per user account.

Why this order matters:

If arg_max() is placed before the where clause, the summarization would occur over all events first, not just 4624, producing incorrect results.

Therefore, the correct logical order is to filter first (where EventID == 4624), and then summarize (arg_max (TimeGenerated, *) by Account).

Alternative incorrect options explained:

summarize make_list(Account) or make_set(Account) by EventID # These aggregate account names for each EventID, not the most recent event per account.

Placing where EventID == 4624 after summarize # Filters after aggregation, which won't return correct results per account.

NEW QUESTION: 61

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You have a query that contains the following statements.

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

You need to configure a custom detection rule that will use the query. The solution must minimize how long it takes to be notified about events that match the query.

Which frequency should you select for the rule?

- A. Continuous (NRT)
- B. Every hour
- C. Every 12 hours
- D. Every 3 hours

Answer: (SHOW ANSWER)

The query filters on ingestion_time() > ago(1d) , which means it is interested in recently ingested device telemetry (DeviceEvents and DeviceProcessEvents) within the last 24 hours. To minimize the time between an event ingest and a detection/notification, you want the rule engine to evaluate the query as close to real- time as possible. Microsoft's XDR/Defender detection framework supports continuous (near-real-time, NRT) detection mode, which evaluates incoming telemetry continuously (or at very short intervals) rather than waiting for a scheduled run.

Scheduled analytics/detection rules run on fixed intervals (for example every hour, every 3 hours, etc.), which introduces a guaranteed latency equal to the schedule period. By contrast, a Continuous (NRT) rule processes telemetry as it arrives (or in very short batch windows), dramatically reducing the time-to-alert for matching events. That makes Continuous (NRT) the correct choice when the requirement is to minimize notification latency for device events.

Note the operational trade-offs: continuous rules can generate more frequent evaluations and higher operational overhead (and potentially more noise), so they should be scoped and tuned appropriately (filters, distinct counts, thresholds) to avoid excessive alerts.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (**415 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You have the hunting query shown in the following exhibit.

```

1 AuditLogs
2 where TimeGenerated > ago(7d)
3 where OperationName == "Add user"
4 project AddedTime, TimeGenerated, user = toString(TargetResources[0].userPrincipalName)
5 join (AzureActivity
6 where OperationName == "Create role assignment"
7 project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
8 project-away user1
9

```

The users perform the following actions:

- * User1 assigns User2 the Global Administrator role.
- * User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
- * User2 creates a new user named User4 and assigns the user the Security Reader role.
- * User2 creates a new user named User5 and assigns the user the Security Operator role.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

NNY

NEW QUESTION: 63

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

What should you do?

- A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.
- B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.

C. From Regulatory compliance, download the report.

D. From Recommendations, download the CSV report.

Answer: ([SHOW ANSWER](#))

In Azure Security Center (now integrated into Microsoft Defender for Cloud), when you receive a security alert, you can view details and recommended remediation actions directly within the portal.

According to Microsoft documentation, each alert in Security Center provides two main sections when you choose Take Action:

- * Mitigate the threat - steps to remediate the immediate incident.

- * Prevent future attacks - recommendations generated by Defender for Cloud to strengthen your security posture and avoid similar alerts in the future.

To specifically view recommendations to resolve the alert, you expand the Prevent future attacks section.

This section includes actionable insights such as enabling Just-In-Time (JIT) VM access, applying system updates, adjusting network security group rules, or enabling endpoint protection.

Other options are incorrect:

- * The Mitigate the threat section focuses on immediate containment, not preventive recommendations.

- * Regulatory compliance and Recommendations pages are general assessments, not alert-specific recommendations.

Therefore, the correct answer is A - select the alert # Take Action # expand Prevent future attacks.

NEW QUESTION: 64

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

A. Yes

B. No

Answer: A ([LEAVE A REPLY](#))

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

NEW QUESTION: 65

You have a Microsoft Sentinel workspace that contains an Azure AD data connector.

You need to associate a bookmark with an Azure AD-related incident.

What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the: Blade

Associate a bookmark with the incident by using the: Blade

Answer:

Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the: Logs blade

Associate a bookmark with the incident by using the: Incident blade

Explanation:

In Microsoft Sentinel, a bookmark is a saved record of an event or query result that an analyst can use to support investigations. Bookmarks are typically created during proactive threat hunting or investigation activities to capture and retain evidence for later correlation or incident enrichment.

According to Microsoft's Sentinel documentation, the Hunting blade provides a workspace where analysts can run Kusto Query Language (KQL) queries across data sources to identify anomalies or suspicious activity. When a suspicious event or pattern is found, the analyst can create a bookmark directly from the Hunting blade. This bookmark stores query details, time range, and contextual information for use in later investigations.

Once the bookmark exists, it can be associated with a specific incident within Sentinel. This association occurs through the Incident blade, where analysts manage alerts, incidents, and investigation details. From the Incident blade, you can attach or link existing bookmarks to provide additional evidence or context, enriching the investigation record and improving traceability within the incident management lifecycle.

In summary:

- * Hunting blade # Used to create bookmarks from proactive searches or hunting queries.
- * Incident blade # Used to associate bookmarks with ongoing incidents for investigation correlation.

Therefore, the correct sequence is:

Create a bookmark using the Hunting blade, and associate it with the incident using the Incident blade.

NEW QUESTION: 66

You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

You need to delegate the following tasks:

* Enable Microsoft Defender for Servers on virtual machines.

* Review security recommendations and enable server vulnerability scans.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Answer Area Task

User

Enable Microsoft Defender for Servers on virtual machines:

User1

Review security recommendations and enable server vulnerability scans:

User1

* Query successful

This is a role-based access control (RBAC) question using the principle of least privilege.

The table of users and roles is:

Name

Role

User1

Security administrator

User2

Security reader

User3

Contributor

Export to Sheets

* Action: This is a management/configuration task at the subscription level, often related to enabling Defender plans and installing extensions on VMs.

* Required Permissions: The ability to modify security policies and settings in Microsoft Defender for Cloud and the permission to install extensions on VMs.

* The Security Administrator role is explicitly designed for this, granting permissions to manage the security features, policies, and program enrollment (like enabling Defender plans).

* The Contributor role can also perform this by installing the necessary agents and extensions, but it grants broad access to manage all resources, violating the principle of least privilege for a purely security-focused task.

* Least Privilege User: User1 (Security administrator)

* Action: This task has two parts:

* Review security recommendations: This is a read-only action. The Security Reader role is sufficient.

* Enable server vulnerability scans: This means configuring a security feature (Vulnerability Assessment), which requires write access to the security configuration or the resource itself.

* The Security Reader role cannot perform the "enable" action.

* The Security Administrator role has the permissions required to modify security policy and configuration to enable scanning features.

* The Contributor role can also do this, but again, the Security Administrator role is the least privileged for a security-specific configuration change.

* Least Privilege User: Since the entire task includes an "enable" (write) action, we must use the role that can perform both read and write security actions. User1 (Security administrator) is the appropriate choice.

Task Analysis and Role Mapping 1. Enable Microsoft Defender for Servers on virtual machines. 2. Review security recommendations and enable server vulnerability scans.

Answer Area Task

User

Enable Microsoft Defender for Servers on virtual machines:

User1

Review security recommendations and enable server vulnerability scans:

User1

NEW QUESTION: 67

You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.

You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:

* Only include security-sensitive actions by users that are NOT members of the IT department.

* Minimize the number of false positives.

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

SecurityEvent

| where EventID in ("4624","4672")

| where Computer == "SERVER1"

| join kind=inner (

| join kind=fullouter (

| join kind=inner (

| join kind=innerunique (

IdentityInfo

BehaviorAnalytics

IdentityInfo

SecurityEvent

These are the selections for the first missing value.

generated, *) by AccountObjectId) on \$left.SubjectUserSid == \$right.AccountSID

Answer:

Answer Area

SecurityEvent

| where EventID in ("4624","4672")

| where Computer == "SERVER1"

| join kind=inner (

| join kind=fullouter (

| join kind=inner (

| join kind=innerunique (

IdentityInfo

BehaviorAnalytics

IdentityInfo

SecurityEvent

These are the selections for the first missing value.

generated, *) by AccountObjectId) on \$left.SubjectUserSid == \$right.AccountSID

Explanation:

Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
  IdentityInfo
  | summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| where Department != "IT"
```

In Microsoft Sentinel with UEBA enabled, user-enrichment data about identities (such as Department , Title , and Account/SID mappings) is written t o the IdentityInfo table. Microsoft guidance recommends joining your security telemetry (for example, SecurityEvent) with IdentityInfo to filter or scope results by organizational attributes like department. To meet the requirement "only include security-s ensitive actions by users that are NOT members of the IT department" , you enrich the Windows security events with IdentityInfo and then filter Department !~ " IT " (or equivalent).

To minimize noise and duplicated rows when joining many-to-one identity recor ds, Sentinel KQL best practices recommend using join kind=innerunique . This join returns at most one matching row from the right table for each row on the left, which helps reduce false positives that can arise from duplicate or stale identity records whil e still ensuring matches are required (i.e., inner). After enriching, you continue your query logic (for example, restricting to Server1 and the subset of security-sensitive event IDs or an UEBA- derived mapping) to identify only the relevant actions.

There fore, the correct completions are to use join kind=innerunique and join to IdentityInfo to apply the department filter and lower false positives.

NEW QUESTION: 68

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You identify the suspicious emails shown in the following table.

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

In the Microsoft Purview portal, you create the content searches shown in the following table.

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)

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 69

You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.

You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.

How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.



```
"resources": [  
  {  
    "type": "Microsoft.Security/automations",  
    "apiVersion": "2019-01-01-preview",  
    "name": "[parameters('name')]",  
    "location": "[resourceGroup().location]",  
    "properties": {  
      "description": "[format(variables('description'), '{0}', parameters('subscriptionId'))]",  
      "isEnabled": true,  
      "actions": [  
        { "actionType": "LogicApp",  
          "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",  
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('resourceGroupName'),  
            'Microsoft.Logic/workflows/',  
            parameters('app1'), 'manual'), '2019-05-01').value]"  
        }  
      ]  
    }  
  }  
]
```

Answer:

Answer Area

```
"resources": [  
  {  
    "type": "Microsoft.Security/automations",  
    "apiVersion": "2019-01-01-preview",  
    "name": "[parameters('name')]",  
    "location": "[resourceGroup().location]",  
    "properties": {  
      "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",  
      "isEnabled": true,  
      "actions": [  
        { "actionType": "LogicApp",  
          "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",  
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),  
            'Microsoft.Logic/workflows/',  
              parameters('app1'),'manual', '2019-05-01').value)]"  
        }  
      ]  
    }  
  }  
]
```

Explanation:

```

"resources": [
  {
    "type": "Microsoft.Security/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[resourceGroup().location]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('resourceGroupName'),
            'Microsoft.Logic/workflows/',
            parameters('app1'), manual(), '2019-05-01').value)]"
        }
      ]
    }
  }
]

```

To launch a Logic App from a Microsoft Defender for Cloud alert, you create a Defender for Cloud automation resource and attach a Logic App action. In ARM, this is modeled with the resource type `Microsoft.Security/automations`. Its properties include `isEnabled`, `scopes`, `sources` (for alert filters), and `actions` -where `actionType` is `LogicApp`. For Logic App actions, Defender for Cloud needs the Logic App's manual trigger callback URL. The ARM pattern uses:

`listCallbackURL(resourceId(subscriptionId, resourceGroupName, 'Microsoft.Logic/workflows/ < workflowName > /triggers/manual ' ), ' 2019-05-01 ' ).value` Hence, the path segment inserted between `.../workflows/` and the trigger name is `triggers` (because the callback URL is retrieved for the manual trigger of the workflow).

So the two correct selections to wire up `app1` to run when a selected Defender for Cloud alert fires are:

- * Set the ARM resource type to `Microsoft.Security/automations`.
- * In the callback URL construction, append `triggers (... /workflows/ < app1 > /triggers/manual )`.

NEW QUESTION: 70

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and contains a Windows device named `Device1`.

The timeline of `Device1` includes three files named `File1.ps1`, `File2.exe`, and `File3.dll`.

You need to submit files for deep analysis in Microsoft Defender XDR.

Which files can you submit?

- A. `File1.ps1` only
- B. `File2.exe` only
- C. `File3.dll` only
- D. `File2.exe` and `File3.dll` only
- E. `File1.ps1` and `File2.exe` only
- F. `File1.ps1`, `File2.exe`, and `File3.dll`

Answer: (SHOW ANSWER)

Microsoft's documentation states clearly that the Deep analysis feature in Defender for Endpoint supports only PE files (Portable Executable files) - specifically `.exe` and `.dll` binaries. In the "Take response actions on a file" article, Microsoft says:

"Only PE files are supported, including .exe and .dll files." Microsoft Learn That means only File2.exe and File3.dll among your three examples are eligible for deep analysis.

Further, a file's "Deep analysis" is only enabled when the file exists in the Defender backend sample collection or is observed on a supported Windows device. The tool won't support script files like .ps1 (PowerShell scripts) via that deep analysis mechanism.

To break it down:

* File1.ps1 (PowerShell script) is not a PE file, so it cannot be submitted to the deep analysis sandbox that expects an executable or library format.

* File2.exe is a standard executable (PE format) and is valid for deep analysis.

* File3.dll is a dynamic-link library (also PE format) and is likewise valid for deep analysis.

Thus, the only files you can submit for deep analysis in Microsoft Defender XDR are those in the proper PE format - File2.exe and File3.dll.

NEW QUESTION: 71

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk.

What should you do?

A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.

B. Modify the properties of the computer objects listed as exposed entities.

C. Disable legacy protocols on the computers listed as exposed entities.

D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B ([LEAVE A REPLY](#))

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-kerberos-delegation>

NEW QUESTION: 72

Your on-premises network contains an Active Directory Domain Services (AD DS) forest.

You have a Microsoft Entra tenant that uses Microsoft Defender for Identity. The AD DS forest syncs with the tenant You need to create a hunting query that will identify LDAP simple binds to the AD DS domain controllers.

Which table should you query?

A. AADServicePrincipalRiskEventi

B. IdentityLogonEvents

C. AADDomainServicesAccountLogon

D. Signinlogs

Answer: (SHOW ANSWER)

In Microsoft Defender for Identity (MDI) , data collected from Active Directory Domain Serv ices (AD DS) is stored in Microsoft 365 Defender advanced hunting tables under the Identity schema.

When investigating LDAP or authentication activities related to domain controllers, the correct table is IdentityLogonEvents .

The IdentityLogonEvents table contains information about all logons detected by Defender for Identity sensors on domain controllers - including LDAP binds , Kerberos , NTLM , and other authentication types.

You can identify LDAP simple binds using a query such as:

IdentityLogonEvents

| wh ere Protocol == " LDAP "

| where AuthenticationPackage == " SimpleBind "

Other options explained:

- * AADServicePrincipalRiskEvents - Contains Entra (Azure AD) service principal risk detections, not AD DS activity.
 - * AADDomainServicesAccountLogon - Used for Azure AD Domain Services (AAD DS), not traditional on-prem AD DS.
 - * SigninLogs - Contains Entra (Azure AD) sign-in data, not LDAP or on-prem authentication.
- # Correct table: IdentityLogonEvents

NEW QUESTION: 73

You have an Azure subscription that contains a Microsoft Sentinel workspace named WS1 and 100 virtual machines that run Windows Server. You need to configure the collection of Windows Security event logs for ingestion to WS1. The solution must meet the following requirements:

- * Capture a full user audit trail including user sign-in and user sign-out events.
- * Minimize the volume of events.
- * Minimize administrative effort.

Which event set should you select?

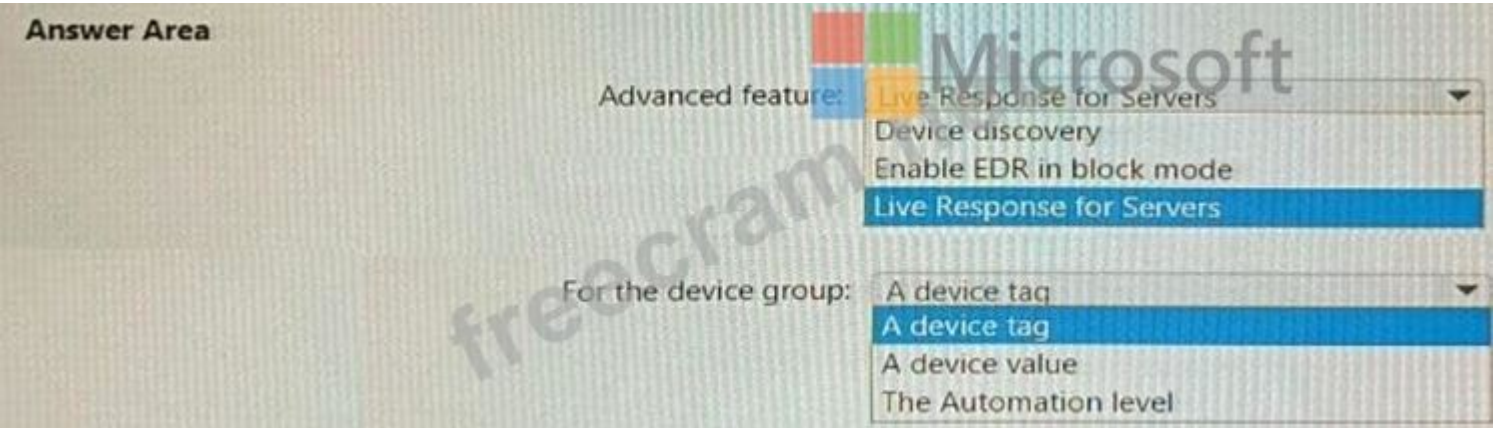
- A. All events
- B. Custom
- C. Minimal
- D. Common

Answer: (SHOW ANSWER)

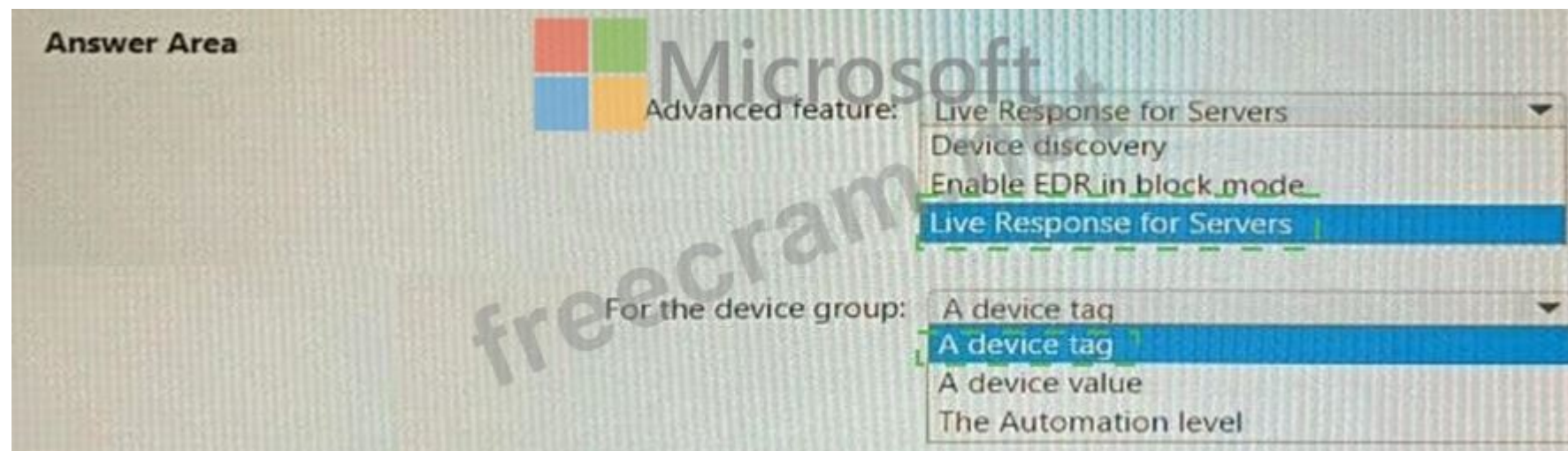
The Common event set is designed to provide a full user audit trail while reducing volume versus "All events." It includes both sign-in (4624) and sign-out/logoff (4634) events. The Minimal set omits sign-out (and other audit events), so it wouldn't meet the requirement; Custom adds admin overhead, and All events increases volume unnecessarily.

NEW QUESTION: 74

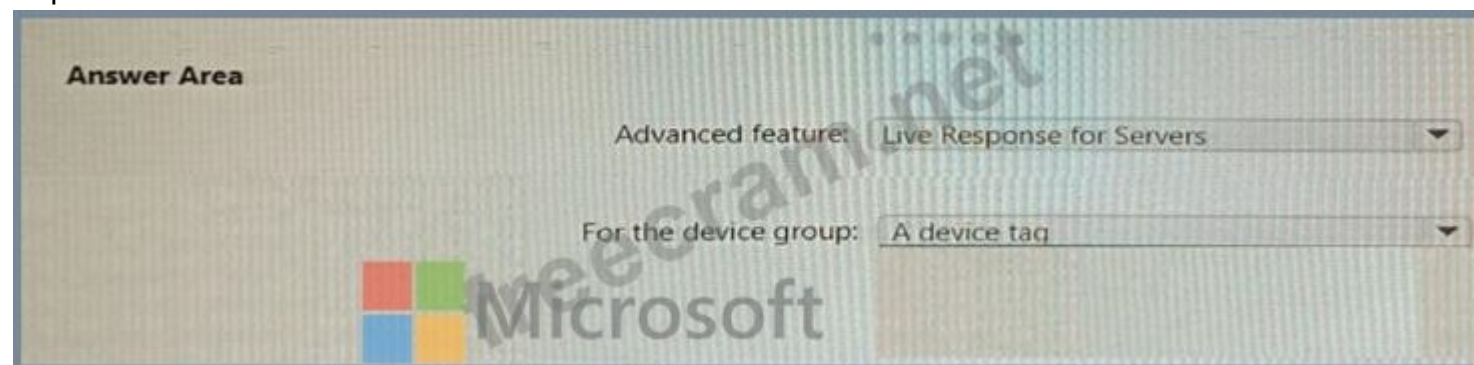
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint. You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



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 Defender 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 Servers" 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 advanced 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

NEW QUESTION: 75

You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.

Which roles should you assign to Used? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD role:

Azure role:

Answer:

Answer Area

Azure AD role:

Azure role:

Explanation:

Answer Area

Azure AD role:

Azure role:

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

NEW QUESTION: 76

You have a Microsoft Sentinel workspace named Workspacel that contains a table named CommonSecurityLog. You ingest logs into CommonSecurityLog. CommonSecurityLog has an average log ingestion time of five minutes.

You need to create an analytics rule that has a lookback period of seven minutes and uses the data in the CommonSecurityLog table. The solution must meet the following requirements:

- * Prevent the same event from being processed twice.
- * Minimize the number of missed events due to log ingestion delays.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

(ingestion_delay + rule_look_back)

(ingestion_delay)

(rule_look_back)

(ingestion_delay + rule_look_back)

(ingestion_delay)

(ingestion_delay)

(rule_look_back)

(ingestion_delay + rule_look_back)

Answer:

Answer Area

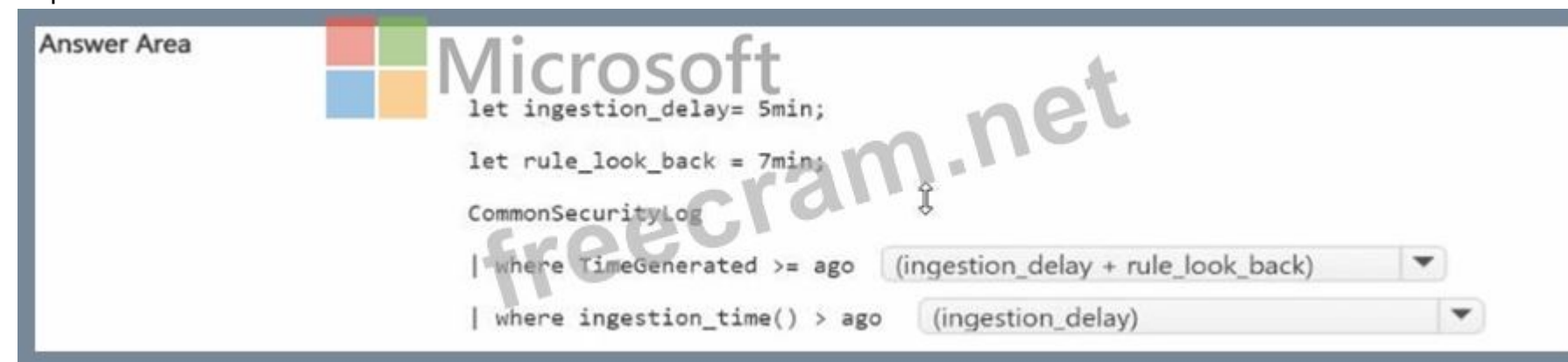


The screenshot shows the Microsoft Sentinel query editor. The query is as follows:

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

Two dropdown menus are visible. The first dropdown, for the `TimeGenerated` filter, has three options: `(ingestion_delay)`, `(rule_look_back)`, and `(ingestion_delay + rule_look_back)`. The second dropdown, for the `ingestion_time()` filter, also has three options: `(ingestion_delay)`, `(rule_look_back)`, and `(ingestion_delay + rule_look_back)`. Both dropdowns have the `(ingestion_delay + rule_look_back)` option selected and highlighted in blue.

Explanation:



The screenshot shows the Microsoft Sentinel query editor with the following query:

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

The dropdown menus are set to `(ingestion_delay + rule_look_back)` for the first filter and `(ingestion_delay)` for the second filter.

When creating scheduled analytics rules in Microsoft Sentinel, you should account for ingestion delay so late-arriving events aren't missed, while also avoiding reprocessing the same events. The recommended pattern is to widen the TimeGenerated window by the expected delay and then gate results by ingestion_time() to include only data that actually arrived within the delay window:

```
let ingestion_delay = 5min;
```

```
let rule_look_back = 7min;
```

```
CommonSecurityLog
```

```
| where TimeGenerated >= ago(ingestion_delay + rule_look_back) // cover late arrivals
```

```
| where ingestion_time() > ago(ingestion_delay) // only newly ingested data
```

* `TimeGenerated >= ago(ingestion_delay + rule_look_back)` ensures the query looks back $7 + 5 = 12$ minutes, so events that were generated up to 7 minutes ago but arrived up to 5 minutes late are still captured.

* `ingestion_time() > ago(ingestion_delay)` limits results to items ingested in the last 5 minutes, preventing the same already-processed events from being picked up again on the next run, while minimizing misses due to late ingestion.

Thus, choose `(ingestion_delay + rule_look_back)` for the first blank and `(ingestion_delay)` for the second.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (**415 Q&As Dumps, 35%OFF Special Discount Code: freecram**)

NEW QUESTION: 77

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: (SHOW ANSWER)

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.

NEW QUESTION: 78

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

- A.** Key Vault firewalls and virtual networks
- B.** Azure Active Directory (Azure AD) permissions
- C.** role-based access control (RBAC) for the key vault
- D.** the access policy settings of the key vault

Answer: (SHOW ANSWER)

When Azure Defender for Key Vault (now Microsoft Defender for Key Vault) detects unauthorized access attempts-especially from Tor exit nodes or other suspicious IPs-the recommended mitigation is to restrict access to trusted networks by using Key Vault firewalls and virtual networks. Microsoft's official guidance specifies: "Enable Key Vault firewalls and virtual networks to allow access only from specific public IP addresses, IP ranges, or selected virtual networks. Deny requests from untrusted sources such as Tor exit nodes." While Azure AD permissions and RBAC control who can authenticate and what operations they can perform, they do not prevent network-level threats. Access policies define granular permissions but cannot block specific network origins. Network-level controls like firewalls and VNets provide the strongest protection against malicious traffic or automated attacks from anonymous sources.

Therefore, to mitigate unauthorized access attempts coming from Tor exit nodes, the appropriate configuration is A. Key Vault firewalls and virtual networks.

NEW QUESTION: 79

You have a Microsoft Sentinel workspace.

You enable User and Entity Behavior Analytics (UEBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:

- * App name: App1
- * IP address: 192.168.1.2
- * Computer name: Device1
- * Used client app: Microsoft Edge
- * Email address: user1@company.com
- * Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

- A. app name, computer name, IP address, email address, and used client app only
- B. IP address and email address only
- C. used client app and app name only
- D. IP address only

Answer: ([SHOW ANSWER](#))

Microsoft Sentinel UEBA (User and Entity Behavior Analytics) focuses on users and hosts (devices) and enriches data with contextual information.

When enabling UEBA with Audit logs and Signin logs, the only entities supported for investigation are:

- * User accounts (email addresses)
- * Hosts or devices (including IP addresses)

Other values like App name, Used client app, and Sign-in URL are attributes in log data but not tracked entities in UEBA investigations.

Answer: B. IP address and email address only

NEW QUESTION: 80

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

Which three 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.

Actions

- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.
- Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
- Download and install the Log Analytics agent.
- Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

Answer:

Actions

- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.
- Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
- Download and install the Log Analytics agent.
- Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

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

Explanation:

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

Reference:

For CEF ingestion, Microsoft Sentinel uses a Linux "log forwarder" that runs the Log Analytics agent (OMS agent) and a syslog daemon (rsyslog/syslog-ng). The documented deployment flow is: first install the Log Analytics agent on the forwarder and connect it to your Sentinel workspace (Workspace ID/Key). Next, configure the agent to listen on TCP/UDP port 25226 -the port the OMS agent uses to receive CEF- translated syslog messages locally-and forward them to the connected workspace (this forwarding is inherent once the agent is connected). Then configure the syslog daemon to receive the external product's CEF events on the chosen syslog port (commonly 514) and forward them locally to 127.0.0.1:25226 . Finally, restart rsyslog/syslog-ng and the OMS agent to apply changes. You do not forward events "directly to Sentinel" from syslog; the agent handles transport to the workspace. An OMS Gateway is only required when the forwarder has no direct Internet access and isn't part of the standard, minimal-effort path. This sequence ensures reliable, supported ingestion of CEF messages into Microsoft Sentinel with the least administrative overhead.

NEW QUESTION: 81

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

- A. Modify the properties of the connector.
- B. Create a Data Collection Rule (DCR).
- C. Create a scheduled query rule.
- D. Enable User and Entity Behavior Analytics (UEBA)

Answer: ([SHOW ANSWER](#))

The core requirement is to customize details included when an alert is created for a specific event. In Microsoft Sentinel, the most effective and granular way to enrich, map, and customize alert fields is by using a Scheduled Query Rule within the Analytics section.

Customization for Microsoft Defender Alerts

* Defender for Cloud Data Connector: This connector, categorized as a Microsoft Security rule type, automatically imports alerts and incidents generated by Microsoft Defender for Cloud into the Microsoft Sentinel SecurityAlert table. These imported alerts have a predefined schema and initial set of details.

* Customization Limitation: You cannot modify the alert schema or customize the details directly on the Microsoft Defender for Cloud data connector itself (Option A).

* Scheduled Query Rule for Enrichment: To customize the alert details, an analyst must run a custom Kusto Query Language (KQL) query against the ingested security alerts (in the SecurityAlert table) or related raw log events. This query is packaged within a Scheduled Query Rule (Option C).

The Role of a Scheduled Query Rule

Scheduled query rules provide the necessary Alert enrichment features to customize alert properties:

* Custom Details (Surface Custom Event Details): This feature allows an analyst to pull any field from the KQL query result and display it prominently in the resulting Sentinel alert and incident.

* Customize Alert Details: This feature allows an analyst to override the default properties of the alert, such as:

* Alert Name Format : Dynamically change the alert title to include specific event values (e.g., Alert from {{ProviderName}}: {{AccountName}} failed to sign in to computer{{ComputerName}}).

* Alert Description Format : Embed custom messages or specific log data into the description.

* AlertSeverity, Tactics, ConfidenceScore, AlertLink , and other key fields: Use values from the query results to set these properties dynamically for each alert instance.

By creating a scheduled query rule that specifically queries the Defender for Cloud alerts and uses KQL to extract or calculate the required custom information, an analyst can then apply the Alert details and Custom details features on the rule 's Set rule logic tab to meet the customization requirement.

NEW QUESTION: 82

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: (SHOW ANSWER)

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.

NEW QUESTION: 83

You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled.

All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud logs to a syslog server.

The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer:

Export logs to: # Azure event hub

* Configure streaming by: # Configuring continuous export in Defender for Cloud for each subscription In Microsoft Defender for Cloud , if you need to stream security alerts and recommendations to an external SIEM or syslog server , the supported approach is to export data to an Azure Event Hub , which acts as a streaming pipeline. The syslog server or SIEM solution can then pull data from the Event Hub in real time using connectors or custom listeners.

The configuration method for sending Defender for Cloud data to an Event Hub is known as continuous export . According to Microsoft's official Defender for Cloud documentation, continuous export lets you automatically stream alerts and security recommendations to Event Hubs or Log Analytics workspaces .

However, when your target is a syslog server , Event Hub is required because it supports continuous streaming outside Azure.

To minimize administrative effort across multiple subscriptions (100 in this case) , you can use Azure Policy or a script to apply continuous export settings per subscription , but the feature must still be enabled individually for each subscription - hence the correct configuration step is:

"Configuring continuous export in Defender for Cloud for each subscription." Why not other options:

* Log Analytics workspace: used for querying within Azure, not for streaming to external syslog servers.

* Azure Storage account: suitable for archival, not streaming.

* Modifying diagnostic settings of the tenant: applies only to Azure AD logs, not Defender for Cloud data.

NEW QUESTION: 84

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.

B. Create a JSON file based on the DNS template.

C. Create an XML file based on the DNS template.

D. Create a YAML file based on the DNS template.

Answer: ([SHOW ANSWER](#))

ASIM parsers in Microsoft Sentinel are stored and deployed as YAML-based content files following ASIM schema templates (e.g., DNS, NetworkSession, etc.).

When you have multiple custom parsers (200 in this case), the most efficient way to manage and deploy them is to create a YAML file that defines all parser configurations and then import it into the Sentinel workspace.

YAML is the supported format for ASIM parser templates in Sentinel's content hub and GitHub deployment model.

Hence, the correct first step is to create a YAML file based on the DNS schema template.

NEW QUESTION: 85

You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks

B. Azure Automation runbooks

C. Microsoft Sentinel automation rules

D. Microsoft Sentinel playbooks

E. Azure Functions apps

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 86

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 87

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.

B. Create a query that uses the workspace expression and the union operator.

C. Use the alias statement.

D. Create a query that uses the resource expression and the alias operator.

E. Add the Azure Sentinel solution to each workspace.

Answer: ([SHOW ANSWER](#))

To hunt across multiple subscriptions/workspaces from a single Microsoft Sentinel workspace, you don't need to re-ingest data; you can query it where it already lives using cross-workspace queries. In KQL, this is done with the workspace() expression combined with union to stitch results from several workspaces in one result set (for example: union workspace('WS1').SecurityEvent, workspace('WS2').SecurityEvent ...). This approach is the supported method for hunting across many projects/subscriptions while keeping data in its original Log Analytics workspaces, and it avoids duplicating ingestion or moving data. In addition, to integrate those remote workspaces with Sentinel features and ensure consistent schema/solution components, you add the Microsoft Sentinel solution to each workspace you want to include. Installing the solution enables Sentinel's content pack, schemas, and permissions model on those workspaces so they can fully participate in Sentinel scenarios while you run cross-workspace hunts from your central workspace. Therefore: (B) Create a query that uses the workspace expression and the union operator and (E) Add the Azure Sentinel solution to each workspace.

NEW QUESTION: 88

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You are investigating an incident.

You need to review the incident tasks that were performed. The solution must include a query that will display the incidents in a workbook, and then display the tasks of each incident in another grid.

Which table should you target in the query?

A. SecurityIncident

B. SecurityEvent

C. SentinelAudit

D. SecurityAlert

Answer: ([SHOW ANSWER](#))

In Microsoft Defender XDR (and Microsoft Sentinel), the table that stores information about incidents- including their status, severity, classification, associated alerts, and related tasks-is the SecurityIncident table. This table is part of the advanced hunting schema and Microsoft Sentinel workspace schema when Microsoft Defender XDR incidents are synchronized to Log Analytics.

Microsoft's documentation for the SecurityIncident table describes it as:

"Contains information about incidents generated in Microsoft Sentinel or Microsoft 365 Defender, including incident title, ID, description, severity, provider, owner, and related entities. It can be used to track and analyze incidents and their associated alerts or tasks." When you need to display incidents in a workbook and also visualize incident tasks or actions performed under each one, you must query the SecurityIncident table. From there, you can join or expand incident details such as tasks or alert relationships for deeper investigation.

Other options are not suitable for this requirement:

* SecurityEvent - contains raw Windows event log data (e.g., logon events, process creation) and is unrelated to incident-level information.

* SentinelAudit - contains audit trail records of changes and administrative actions within Sentinel (e.g., who modified analytics rules), not incidents or tasks.

* SecurityAlert - contains individual alerts that may belong to incidents, but it doesn't include incident tasks or groupings by incident.

Therefore, to query incident information and related tasks in a workbook, the correct target table is SecurityIncident .

NEW QUESTION: 89

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A. the Azure Active Directory Provisioning Analysis workbook

B. the Overview settings of Insider risk management

C. the Modifications of sensitive groups report in Microsoft Defender for Identity

D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Answer: ([SHOW ANSWER](#))

In a Microsoft 365 E5 subscription with a hybrid Azure AD environment , monitoring changes to privileged Active Directory groups (like Domain Admins) is handled by Microsoft Defender for Identity . The "Modifications of sensitive groups" report provides visibility into all changes made to sensitive AD groups such as Domain Admins , Enterprise Admins , and Schema Admins .

According to Microsoft Defender for Identity documentation:

"The Modifications of sensitive groups report identifies all changes to highly privileged groups, including additions and removals of members. It helps detect potential privilege escalation and insider threats." This report displays all relevant group modification activities within a defined time range (for example, the last 30 days), fulfilling the requirement.

Correct answer: C. the Modifications of sensitive groups report in Microsoft Defender for Identity

NEW QUESTION: 90

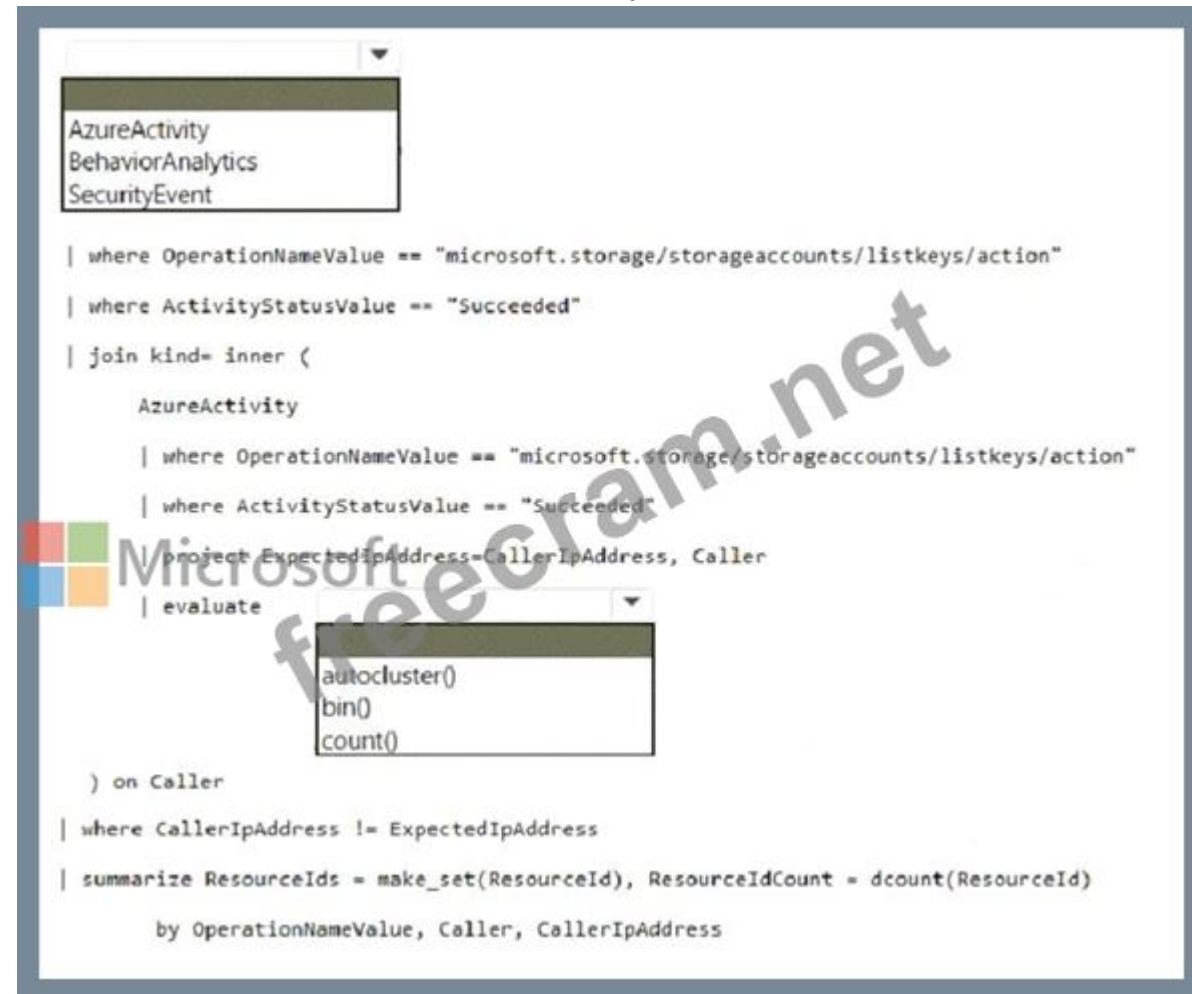
You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts.

The solution must exclude users that list storage keys for a single storage account.

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

NOTE: Each correct selection is worth one point.



The screenshot shows a KQL query in the Microsoft Sentinel workspace 'sws1'. The query is designed to identify users who list storage keys for multiple Azure Storage accounts, while excluding those who only list keys for a single account. The query uses the 'AzureActivity' table and filters for 'microsoft.storage/storageaccounts/listkeys/action' operations that have succeeded. It joins the main query with a subquery that also filters for the same action and status. The query then projects the 'ExpectedIpAddress' and 'Caller' fields and evaluates the 'autocluster()' function. Finally, it filters for callers where the 'CallerIpAddress' is not equal to the 'ExpectedIpAddress' and summarizes the results by 'OperationNameValue', 'Caller', and 'CallerIpAddress'.

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

Answer:



```
| 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()
        bin()
        count()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
    by OperationNameValue, Caller, CallerIpAddress
```

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

AzureActivity

```
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
```

```
| where ActivityStatusValue == "Succeeded"
```

```
| join kind= inner (
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set (ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller,
CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous\_Listing\_Of\_Storage\_Keys.yaml
```

NEW QUESTION: 91

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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

NOTE: Each correct selection is worth one point

```
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( DstGeoCountry
SrcGeoCountry
SrcGeoRegion
) by TargetUserId, TargetUserPrincipalName, TargetUserType

| where NumOfCountries >= threshold
```



Microsoft

imAuthentication

imAuthentication

imNetworkSession

imProcessCreate

imWebSession

DstGeoCountry

SrcGeoCountry

SrcGeoRegion

Answer:

```
let timeframe = ago(3h);
```

```
let threshold = 5;
```

imAuthentication
imAuthentication
imNetworkSession
imProcessCreate
imWebSession

```
| 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( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
```

```
| where NumOfCountries >= threshold
```

Explanation:

```
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
```

Below is the completed KQL that meets the requirement (successful sign-ins from multiple countries in the last 3 hours), using the ASIM authentication 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 logons.

* 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 delivers 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.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 92

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

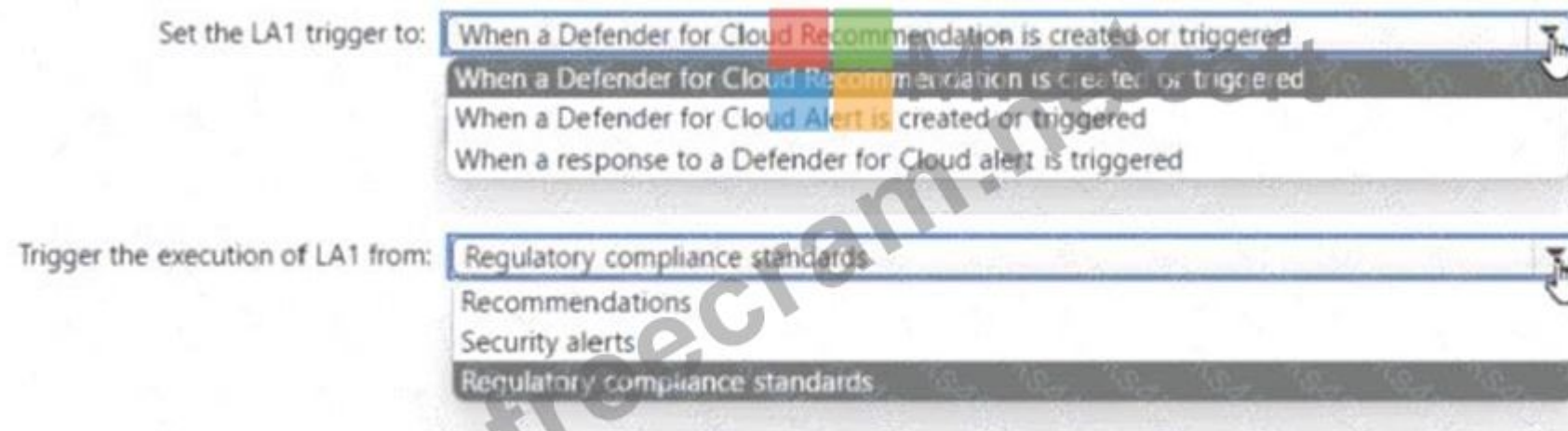
You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud .

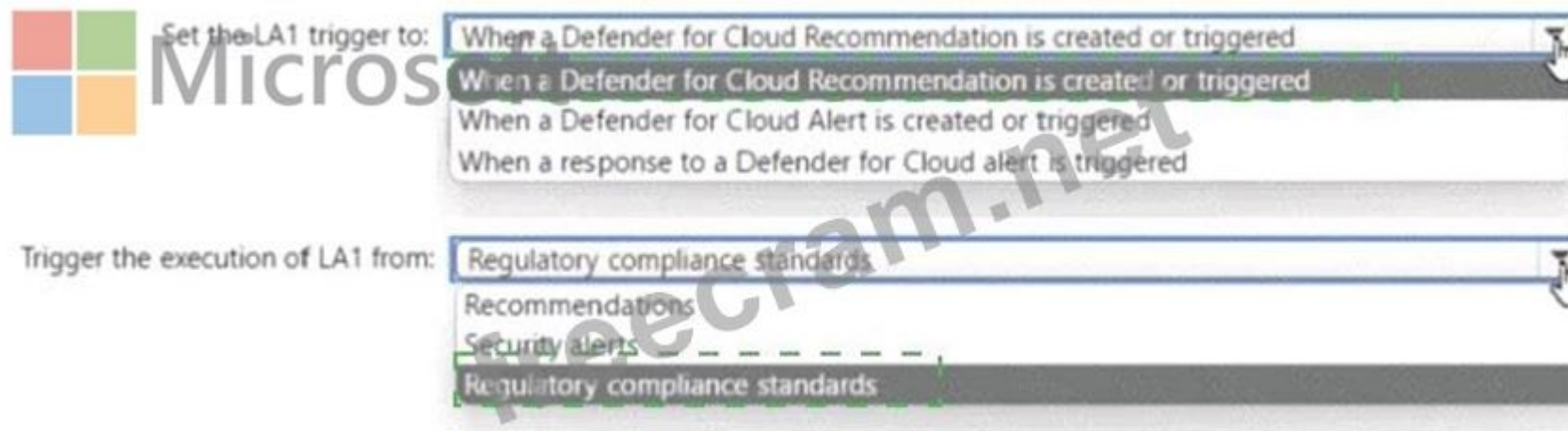
You need to test LA1 in Defender for Cloud .

What should you do? To answer, select the appropriate options in the answer area.

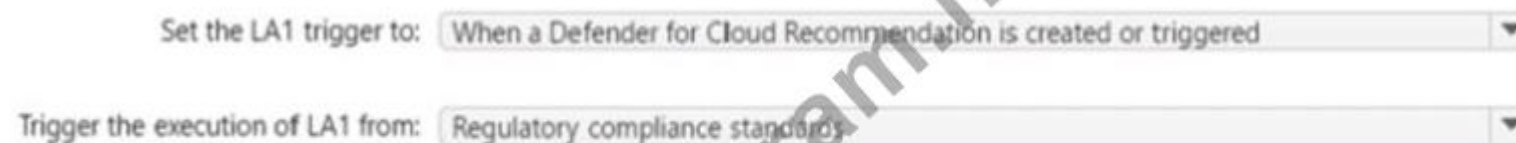
NOTE: Each correct selection is worth one point.



Answer:



Explanation:



According to Microsoft Defender for Cloud automation documentation, Logic Apps can be integrated to automatically respond to recommendations or alerts. To test or automate remediation from Defender for Cloud, you must configure an automation workflow (Logic App) that triggers when a recommendation is created or updated.

Microsoft defines the available triggers for Defender for Cloud automation as follows:

- * When a Defender for Cloud Recommendation is created or triggered - This event type initiates the Logic App whenever a new security recommendation appears or an existing one changes state. It's the proper trigger for remediation scenarios because recommendations typically indicate a detected security misconfiguration or risk requiring action.
- * When a Defender for Cloud Alert is created or triggered - This applies to security alerts, not recommendations.
- * When a response to a Defender for Cloud alert is triggered - Used for incident-response workflows, not for testing remediation logic.

In the context of the question, the goal is to test automatic remediation for detected configuration issues (security risks). Those are surfaced as recommendations within Defender for Cloud, not as alerts.

Next, the execution source should be configured under:

- * Trigger the execution of LA1 from: Recommendations

This ensures that Defender for Cloud will execute the Logic App (LA1) automatically when relevant recommendations are triggered, allowing immediate testing and validation of the remediation logic.

In summary:

To test the Logic App remediation workflow in Defender for Cloud, you must:

- * Set the trigger type to "When a Defender for Cloud Recommendation is created or triggered" .
- * Configure it to execute from "Recommendations" .

Thus, the verified correct answers are:

- # Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
- # Trigger the execution of LA1 from: Recommendations

NEW QUESTION: 93

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.
From the Microsoft 365 Defender portal, which page should you use to create the query?

- A. Policies & rules
- B. Explorer
- C. Threat analytics
- D. Advanced Hunting

Answer: (SHOW ANSWER)

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 Hunting" 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 analytics - offers intelligence-driven insights and reports but doesn't allow creating custom queries.

Correct answer: D. Advanced Hunting

NEW QUESTION: 94

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
You have a Microsoft Sentinel workspace.
Microsoft Sentinel connectors are configured as shown in the following table.

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

You use Microsoft Sentinel to investigate suspicious Microsoft Graph API activity related to Conditional Access policies. You need to search for the following activities:

- * Downloads of the Conditional Access policies by using PowerShell
 - * Updates to the Conditional Access policies by using the Microsoft Entra admin center
- Which tables should you query for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Conditional Access policy downloads:

Conditional Access policy updates:

Answer:

Answer Area

Conditional Access policy downloads:

Conditional Access policy updates:

Explanation:

Answer Area

Conditional Access policy download:

Conditional Access policy updates:

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-MgIdentityConditionalAccessPolicy`). Those Graph requests 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), and 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 Conditional 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.

NEW QUESTION: 95

You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.

You have a team named Team1 that has a project named Project 1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.

Which KQL query should you run?

A. `(c:c)(Project1)(date=(2023-02-01)..date=(2023-02-10))`

B. `Project1(c:c)(date=2023-02-01..2023-02-10)`

C.

```
AuditLogs
| where Timestamp > ago(10d)
| where FileName contains "Project1"
```

D.

```
AuditLogs
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains "Project1"
```

Answer: (SHOW ANSWER)

According to Microsoft Purview and Kusto Query Language (KQL) documentation, when you need to filter audit or activity logs based on a specific date range, the correct approach is to use the between (datetime())..

datetime()) operator. This operator allows defining a start and end datetime for filtering events. The AuditLogs table is the appropriate data source for searching Microsoft 365 audit events, including file activities in SharePoint and Teams sites.

In this scenario, the goal is to identify all files related to "Project1" stored on the Team1 site between February 1, 2023, and February 10, 2023. The where clause is used to filter the results first by Timestamp (activity date/time) and then by FileName to find the relevant project files.

The correct syntax aligns exactly with the Microsoft KQL documentation pattern:

| where Timestamp between (datetime(StartDate)..datetime(EndDate))

This ensures that only audit records falling within that time window are retrieved.

Other options are incorrect because they either lack valid KQL structure or use unsupported syntax for date ranges. Thus, Option D is the verified answer.

NEW QUESTION: 96

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains two users named User1 and User2.

You need to ensure that the users can perform searches by using the Microsoft Purview portal. The solution must meet the following requirements:

- * Ensure that User1 can search the Microsoft Purview Audit service logs and review the Microsoft Purview Audit service configuration.
- * Ensure that User2 can search Microsoft Exchange Online mailboxes.
- * Follow the principle of least privilege.

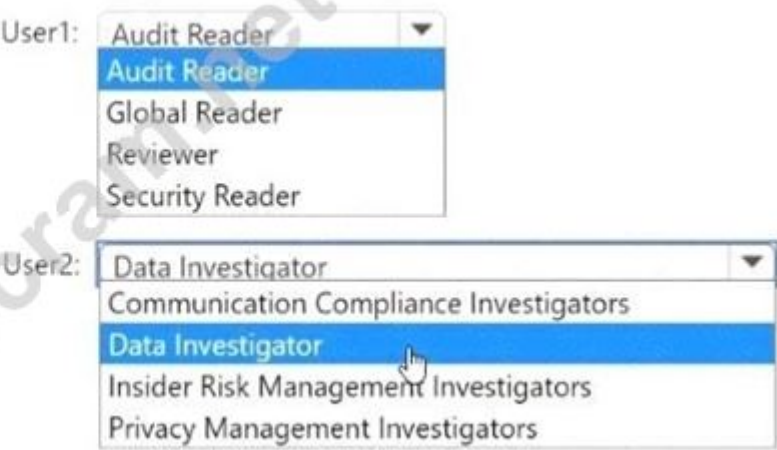
To which Microsoft Purview role group should you add each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1: Audit Reader

User2: Data Investigator



Answer:



Explanation:



In Microsoft Purview, permissions to perform searches, audits, and investigations are managed through role groups within the Microsoft Purview compliance portal. Each role group provides specific capabilities aligned with least privilege principles.

User1 - Search Audit Logs and Review Configuration To allow a user to:

- * Search the Microsoft Purview Audit logs, and
 - * Review the Audit configuration and settings,
- ...the required role group is Audit Reader.

According to Microsoft documentation:

"Members of the Audit Reader role group can search the audit log for user and admin activities and view audit configuration settings." This group grants audit-related permissions only - it does not grant access to other Purview or mailbox content, meeting the least privilege requirement.

User1 = Audit Reader

User2 - Search Exchange Online Mailboxes To allow a user to:

- * Perform content searches across Microsoft Exchange Online mailboxes,
- ...the correct role group is Data Investigator.

Per Microsoft Purview documentation:

"Members of the Data Investigator role group can perform content searches across Exchange Online, SharePoint Online, and OneDrive locations." Other options such as Communication Compliance Investigators or Insider Risk Management Investigators are specific to their respective Purview solutions and not used for general content or mailbox searches.

User2 = Data Investigator

NEW QUESTION: 97

You need to meet the Microsoft Defender for Cloud Apps requirements

What should you do? To answer, select the appropriate options in the answer area.

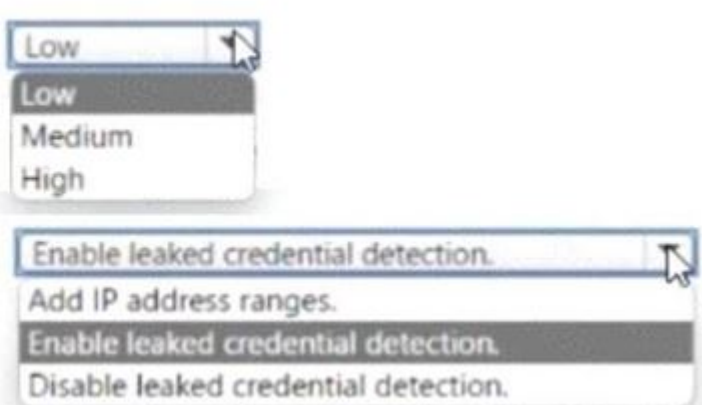
NOTE: Each correct selection is worth one point.

Answer Area

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

To reduce the amount of false positive alerts:

Microsoft



The screenshot shows the configuration interface for impossible travel alert policies. The sensitivity level is set to Low, and the option to enable leaked credential detection is selected. The interface includes a dropdown menu for sensitivity levels (Low, Medium, High) and a list of options to reduce false positive alerts (Enable leaked credential detection, Add IP address ranges, Disable leaked credential detection).

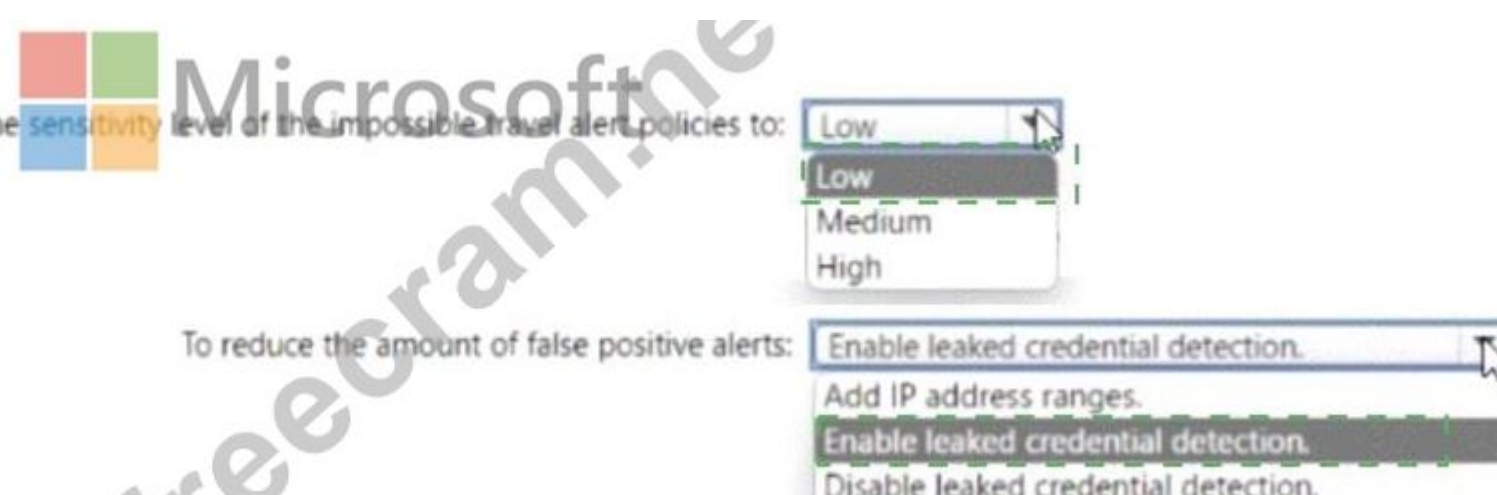
Answer:

Answer Area

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

To reduce the amount of false positive alerts:

Microsoft



The screenshot shows the configuration interface for impossible travel alert policies. The sensitivity level is set to Low, and the option to enable leaked credential detection is selected. The interface includes a dropdown menu for sensitivity levels (Low, Medium, High) and a list of options to reduce false positive alerts (Enable leaked credential detection, Add IP address ranges, Disable leaked credential detection).

Explanation:

Set the sensitivity level of the impossible travel alert policies to: Low To reduce the amount of false positive alerts: Add IP address ranges In Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) , the impossible travel alert policy detects when a user signs in from two geographically distant locations within a timeframe that would make physical travel between them impossible. This is an important indicator of potential account compromise but can also generate false positives if not tuned properly.

* Setting Sensitivity Level to Low: Microsoft Defender for Cloud Apps allows tuning of the Impossible travel policy sensitivity between Low , Medium , and High .

* High sensitivity increases detection but also raises the likelihood of false positives.

* Medium offers a balance.

* Low reduces the number of alerts by limiting detections to only the most obvious and high- confidence anomalies. To meet operational requirements that minimize alert noise and false positives, the sensitivity should be set to Low .

* Reducing False Positives - Add IP Address Ranges: According to Microsoft's official Defender for Cloud Apps policy tuning guidance, the main way to reduce false positives in impossible travel alerts is by adding trusted IP address ranges (e.g., office networks, VPN exit nodes, proxy gateways) to the trusted IPs list . This ensures that logins from corporate or known network ranges are not flagged as anomalous, thereby significantly reducing false alerts.

Other options, like enabling or disabling leaked credential detection, are unrelated to the impossible travel anomaly and affect credential theft alerts instead.

Therefore, the verified correct configuration is:

Sensitivity level: Low

Reduce false positives by: Add IP address ranges

NEW QUESTION: 98

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.

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

NOTE: Each correct selection is worth one point.

Answer Area

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



Answer:



DeviceLogonEvents

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

Explanation:

Answer Area



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

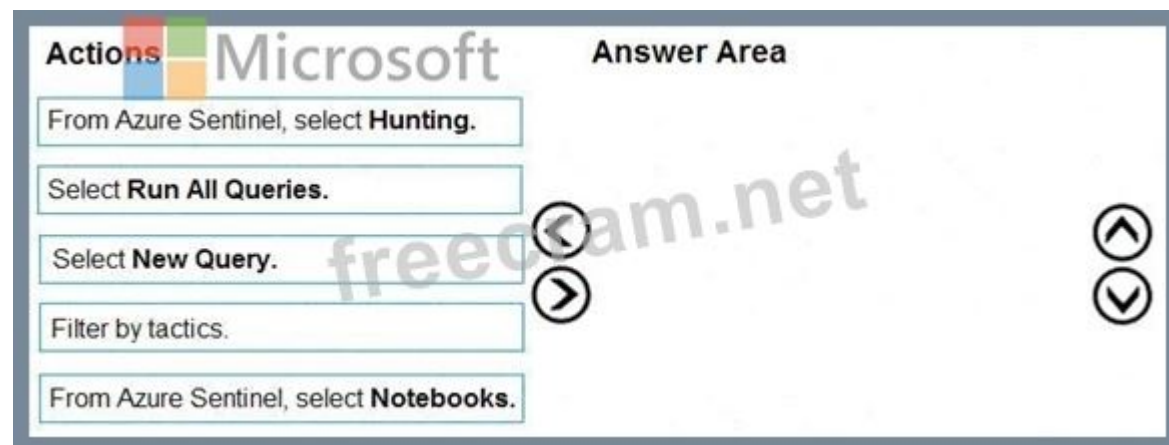
To combine sign-in attempts from endpoints and on-premises AD DS domain controllers in Microsoft 365 Defender advanced hunting, you should query the tables that record those events and union them. DeviceLogonEvents contains interactive and network logon activity collected from devices onboarded to Microsoft Defender for Endpoint, while IdentityLogonEvents contains sign-in activity observed by Microsoft Defender for Identity sensors on domain controllers. Using union 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.

NEW QUESTION: 99

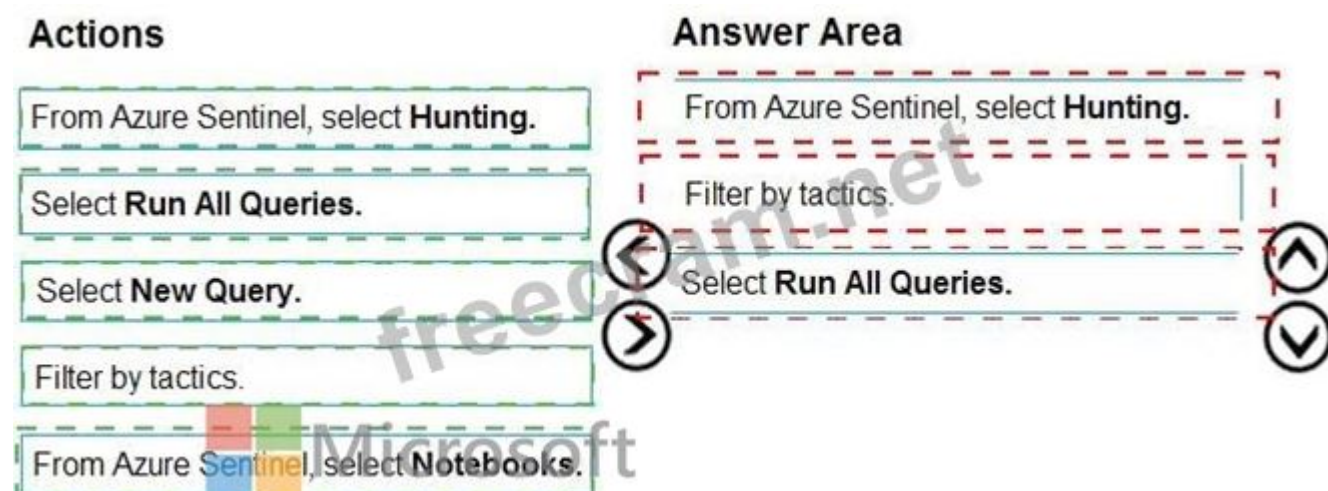
You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

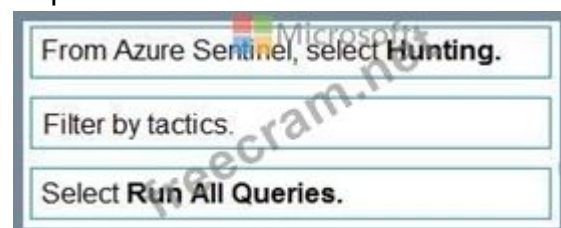
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:



According to Microsoft Sentinel documentation, Hunting is a proactive feature that allows analysts to query raw security data for indicators of compromise (IoCs), suspicious patterns, and potential threats. When an analyst needs to query for suspicious credential access activities, they should use the Hunting page in the Microsoft Sentinel portal.

The correct sequence is as follows:

- * From Azure Sentinel, select Hunting. This step opens the Hunting dashboard, which provides access to all prebuilt and custom hunting queries. Each query corresponds to specific tactics and techniques aligned with the MITRE ATT & CK framework.
- * Filter by tactics. Since the goal is to find suspicious credential access, you should filter the hunting queries by the Credential Access tactic. This narrows the view to only the queries related to credential theft or misuse activities.
- * Select Run All Queries. Once filtered, running all relevant hunting queries executes them against your connected data sources (e.g., Defender for Endpoint, Azure AD logs, etc.) to identify suspicious credential activity patterns.

Why not the other options?

- * Select New Query is used to create a custom hunting query, not to search existing suspicious credential access detections.
- * From Azure Sentinel, select Notebooks is for advanced visualization and correlation using Jupyter, not for tactical hunting queries.

Final Correct Sequence:

From Azure Sentinel, select Hunting

Filter by tactics
Select Run All Queries

NEW QUESTION: 100

You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

Change the alert severity threshold for emails to **Medium**.

Rename the executable file as AlertTest.exe.

Change the alert severity threshold for emails to **Low**.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.

Run the executable file and specify the appropriate arguments.

Answer Area

>

<

^

v

 Microsoft

Answer:

Actions

Enable Microsoft Defender for Cloud's enhanced security features for the subscription.
Change the alert severity threshold for emails to Medium .
Rename the executable file as AlertTest.exe.
Change the alert severity threshold for emails to Low .
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Run the executable file and specify the appropriate arguments.

Answer Area

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Run the executable file and specify the appropriate arguments.
Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

Explanation:

To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:

- * Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe
- * Run the executable file and specify the appropriate arguments
- * Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

NEW QUESTION: 101

You have a Microsoft 365 E5 subscription that uses Microsoft Copilot for Security. You plan to run the following code to create a custom Copilot for Security plugin.

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

You need to specify a format and complete the code segment. Which format should you use for the < target > variable?

- A. API
- B. GPT
- C. KQL
- D. SQL

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 102

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 103

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.

Does this meet the goal?

- A. Yes
- B. No

Answer: B ([LEAVE A REPLY](#))

In Microsoft Defender for Identity (MDI), the goal described - "configure several accounts for attackers to exploit" - refers to creating honeypot accounts. A honeypot is a decoy user account deliberately configured to appear valuable (e.g., privileged or high-value) but is not used by legitimate users. Defender for Identity monitors these accounts, and if any authentication or access attempt is detected, it triggers an immediate alert because such activity indicates potential attacker reconnaissance or compromise.

According to Microsoft Defender for Identity documentation, to designate honeypot accounts, you must explicitly add the accounts themselves under the Honeypot accounts configuration in the MDI portal.

The portal path is:

Defender for Identity Portal # Configuration # Honeypot accounts # Add accounts.

Adding accounts to a Sensitive group does not make them honeytokens. Sensitive groups (like Domain Admins or Enterprise Admins) are used by Defender for Identity to track privileged account activities and detect lateral movement, but they are not monitored as honeypots.

Therefore, while adding accounts to a Sensitive group increases monitoring visibility for privilege abuse, it does not fulfill the goal of configuring specific accounts as decoy targets for attackers.

Hence, the correct and verified answer is B. No - the described solution does not meet the goal.

NEW QUESTION: 104

You have a Microsoft 365 E5 subscription and a Microsoft Sentinel workspace. You need to create a KQL query that will combine data from the following sources:

- * Microsoft Graph

- * Risky users detected by using Microsoft Entra ID Protection

The solution must minimize the volume of data returned. How should the query start?

A. MicrosoftGraphActivityLogs

lookup kind=leftouter AADRiskyUsers on \$left.UserId == \$right.Id

B. MicrosoftGraphActivityLogs

join AADRiskyUsers on \$left.UserId == \$right.Id

C. MicrosoftGraphActivityLogs

join AADUserRiskEvents on \$left.UserId == \$right.Id

D. find in (MicrosoftGraphActivityLogs, AADUserRiskEvents) where

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 105

You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.

You need to create a new near-real-time (NRT) analytics rule that will use the playbook.

What should you configure for the rule?

A. the Incident automation settings

B. entity mapping

C. the query rule

D. the Alert automation settings

Answer: ([SHOW ANSWER](#))

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:

NEW QUESTION: 106

You have an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.

csv that contains 10,000 rows.

You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Excel, you apply filters to the existing columns in File1.csv to reduce the number of rows, and then you perform the Get & Transform Data operations to parse the AuditData column.

Does this meet the requirement?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

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, Power 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.

The 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 the 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.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 107

You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

A. the Dependency agent

B. the Log Analytics agent

C. the Azure Connected Machine agent

D. the Guest Configuration extension

Answer: ([SHOW ANSWER](#))

Defender for Cloud depends on the Log Analytics agent.

Use the Log Analytics agent if you need to:

- * Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure

- * Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage>

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent>

NEW QUESTION: 108

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

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

NOTE: Each correct selection is worth one point.

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

The first dropdown menu (after `distinct DeviceId`) has the following options:

- extend
- join
- project

The second dropdown menu (after `join AlertInfo on AlertId`) has the following options:

- project
- summarize
- take

Answer:

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

Explanation:

Box 1: join
An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.
This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

```
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"
```

Box 2: project

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

NEW QUESTION: 109

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

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

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered.

The solution must minimize administrative effort.
Which three 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.

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.

>

<

1

2

3

Answer Area



Answer:

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.

>

<

1

2

3

Answer Area

Configure the Trigger automated response settings.

Filter by alert title.

Select **Take action**.



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.

You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender.

The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 111

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You manually install the Log Analytics agent on the virtual machines.

Does this meet the goal?

- A. Yes
- B. No

Answer: ([SHOW ANSWER](#))

If you manually install the Log Analytics agent on your AWS Linux VMs and connect them to your Azure Log Analytics workspace, Defender for Cloud can begin collecting telemetry data from those machines.

Once connected, Azure Defender automatically protects and monitors them, even if they are hosted outside Azure.

Microsoft Defender for Cloud documentation explains:

"You can manually install the Log Analytics agent on non-Azure machines and connect them to your workspace. Once connected, Defender for Servers will begin applying protections and generating alerts." Although Azure Arc provides centralized management and auto-provisioning, manually installing the Log Analytics agent is a valid and supported alternative method. Therefore, this solution also meets the goal.

Correct answer: A. Yes

NEW QUESTION: 112

You have an Azure subscription that contains 50 virtual machines.

You plan to deploy Microsoft [Defender for Cloud.

You need to enable agentless scanning for 40 virtual machines. The solution must create disk snapshots of the virtual machines and perform out-of-band analysis of the snapshots.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Select Defender plan: Defender CSPM
Defender CSPM
Resource Manager
Storage

To exclude specific virtual machines, use: Tagging
A role-based access control (RBAC) assignment
An Azure Policy assignment
Tagging

Answer:

Answer Area

Select Defender plan: Defender CSPM
Defender CSPM
Resource Manager
Storage

To exclude specific virtual machines, use: Tagging
A role-based access control (RBAC) assignment
An Azure Policy assignment
Tagging

Explanation:

Answer Area

Select Defender plan: Defender CSPM

To exclude specific virtual machines, use: Tagging

The scenario describes agentless scanning for virtual machines - a feature of Microsoft Defender for Cloud under the Defender CSPM (Cloud Security Posture Management) plan. Defender CSPM introduces agentless scanning capabilities that use snapshot-based (out-of-band) scanning to assess OS vulnerabilities, sensitive data, and configurations without requiring agents .

Microsoft documentation clarifies:

"Agentless scanning for machines is available in Defender CSPM and Defender for Servers P2. The scanning engine takes snapshots of virtual machines and performs analysis out-of-band to identify vulnerabilities and sensitive data exposure." For controlling which virtual machines participate, tag-based inclusion or exclusion is used. You can define which machines to include/exclude using Azure resource tags , such as:

Environment=Production

Scan=Exclude

Microsoft Defender for Cloud reads these tags to determine which resources should have scanning enabled or excluded.

Role-based access control (RBAC) and Azure Policy assignments control access and policy enforcement, but they are not used to exclude specific resources from Defender CSPM agentless scanning.

Final Configuration:

* Defender Plan: Defender CSPM

* Exclusion Method: Tagging

NEW QUESTION: 113

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

- A.** the Azure Storage Analytics logs
- B.** the activity logs of storage1
- C.** the alert details
- D.** the related entities of the alert

Answer: ([SHOW ANSWER](#))

To identify which blobs were deleted in an Azure Storage account, you must review Azure Storage Analytics logs, which record all operations (including DeleteBlob and DeleteContainer requests) made against the storage service.

These logs contain details such as timestamp, requester IP, operation type, and object name-allowing you to pinpoint the exact blobs deleted.

* Activity logs (Option B) record control-plane operations (e.g., resource creation or configuration changes), not data-plane operations like blob deletions.

* Alert details and related entities (Options C and D) summarize detection context but do not include full operation-level details.

Correct answer: A. the Azure Storage Analytics logs

NEW QUESTION: 114

You have a Microsoft 365 E5 subscription.

You need to search the Microsoft Purview audit log by using PowerShell on a Windows device.

What should you do first?

- A.** Modify the TrustedHosts list
- B.** Install the Microsoft Exchange Online PowerShell module.
- C.** Install the Microsoft Graph PowerShell module.
- D.** Enable PowerShell remoting.

Answer: ([SHOW ANSWER](#))

Microsoft Purview audit-log search via PowerShell is performed with Exchange Online cmdlets. Microsoft's guidance states: "Use the Search-UnifiedAuditLog cmdlet to search the audit log for events."

This cmdlet is part of the Exchange Online PowerShell (ExchangeOnlineManagement) module and requires you to connect to the service before running queries. Microsoft further notes that you must install and import the Exchange Online PowerShell V2 module and then connect (for example, Connect-ExchangeOnline) to run compliance and audit-related cmdlets, including Search-UnifiedAuditLog. In short, on a Windows device the first prerequisite is installing the Exchange Online PowerShell module, after which you authenticate and run your audit searches. Alternatives such as enabling remoting or modifying TrustedHosts are unrelated, and the Microsoft Graph PowerShell module does not provide the Search-UnifiedAuditLog cmdlet that Purview audit searches rely on. Therefore, the correct first step is to install the Microsoft Exchange Online PowerShell module.

NEW QUESTION: 115

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You investigate Device1 for malicious activity and discover a suspicious file named File1.exe. You collect an investigation package from Device1.

You need to review the following forensic data points:

- . Is an attacker currently accessing Device1 remotely?
- . When was File1.exe first executed?

Which folder in the investigation package should you review for each data point? To answer, select the appropriate options in the answer area.

Is an attacker currently accessing Device1 remotely:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

When was File1.exe first executed:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

Answer:

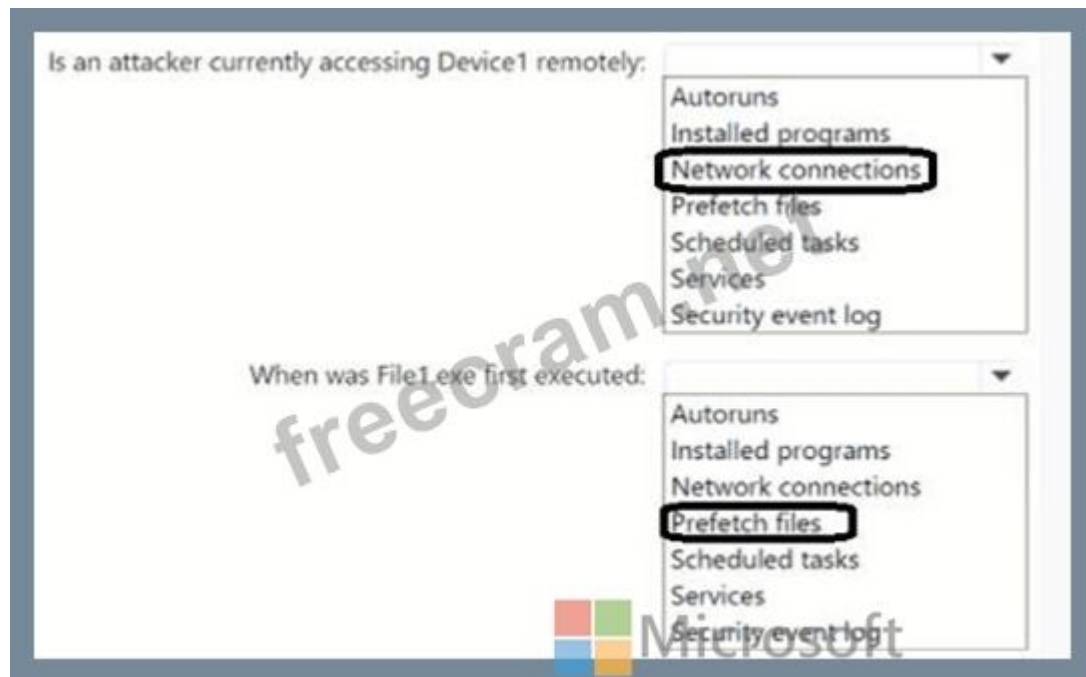
Is an attacker currently accessing Device1 remotely:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

When was File1.exe first executed:

- Autoruns
- Installed programs
- Network connections
- Prefetch files
- Scheduled tasks
- Services
- Security event log

Explanation:



To determine whether a device is being accessed remotely by an attacker, analysts must inspect active network connections collected from the investigation package.

Microsoft Defender for Endpoint investigation packages contain a NetworkConnections.txt file that includes all established, listening, and closed network sessions, including remote IP addresses, ports, and associated processes.

Microsoft's official Defender for Endpoint documentation states:

"The investigation package includes a list of active network connections at the time of collection, helping analysts identify potential remote access activity or suspicious outbound connections." By reviewing the network connections folder/file, you can check for any live sessions to external IPs, RDP, SSH, or other remote-control tools indicating an attacker's presence.

Data Point 2: When was File1.exe first executed?

Verified Answer = Prefetch files

To find when a file was first executed, you use Prefetch files .

Windows Prefetch is a forensic artifact that records metadata about executables that have been launched, including:

- * The first and last execution timestamps
- * The number of times executed
- * The path and hash of the executable

Microsoft's forensic analysis guidance for Defender investigation packages specifies:

"Prefetch files provide information on when applications were first and last executed, which assists in establishing file execution timelines during investigations." Therefore, to determine when File1.exe was first executed, you should analyze the Prefetch files contained within the investigation package.

Final Verified Answers:

Forensic Data Point

Folder/File to Review

Is an attacker currently accessing Device1 remotely?

Network connections

When was File1.exe first executed?

Prefetch files

Summary:

* Network connections # Identify active remote sessions (possible attacker access)

* Prefetch files # Determine first execution time of suspicious executable These answers align with Microsoft Defender for Endpoint investigation package structure and Microsoft 365 E5 SecOps documentation .

NEW QUESTION: 116

You have an on-premises network.

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity.

From the Microsoft Defender portal, you investigate an incident on a device named Device1 of a user named User1. The incident contains the following Defender for Identity alert.

Suspected identity theft (pass-the-ticket) (external ID 2018)

You need to contain the incident without affecting users and devices. The solution must minimize administrative effort.

What should you do?

- A. Disable User 1 only.
- B. Quarantine Device1 only.
- C. Reset the password for all the accounts that previously signed in to Device1.
- D. DisableUser1 and quarantine Device1.
- E. Disable User1, quarantine Device1, and reset the password for all the accounts that previously signed in to Device1.

Answer: (SHOW ANSWER)

According to Microsoft Defender for Identity documentation, when an alert such as "Suspected identity theft (Pass-the-Ticket)" appears, it indicates that a compromised Kerberos ticket might have been used by an attacker to impersonate a legitimate account. The goal in this scenario is to contain the spread of the attack while minimizing disruption to unaffected users and systems.

Microsoft recommends isolating or quarantining the compromised device first, as it is the likely source of the malicious activity. Quarantining Device1 blocks it from communicating with other networked systems, preventing further credential theft or lateral movement, while allowing SOC teams to investigate and remediate the issue.

Resetting all account passwords or disabling user accounts at this stage could cause significant operational disruption and is not advised unless there is evidence that multiple credentials were compromised. Defender for Identity's containment guidance explicitly notes:

* "Contain the affected device to stop further credential theft or movement."

* "Reset passwords only for accounts confirmed to be compromised."

Therefore, the least disruptive and most efficient containment step is to quarantine Device1 only. This action effectively isolates the threat while maintaining normal operations for other users and devices, satisfying the requirement to minimize administrative effort and user impact.

Hence, the verified answer is B. Quarantine Device1 only.

NEW QUESTION: 117

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

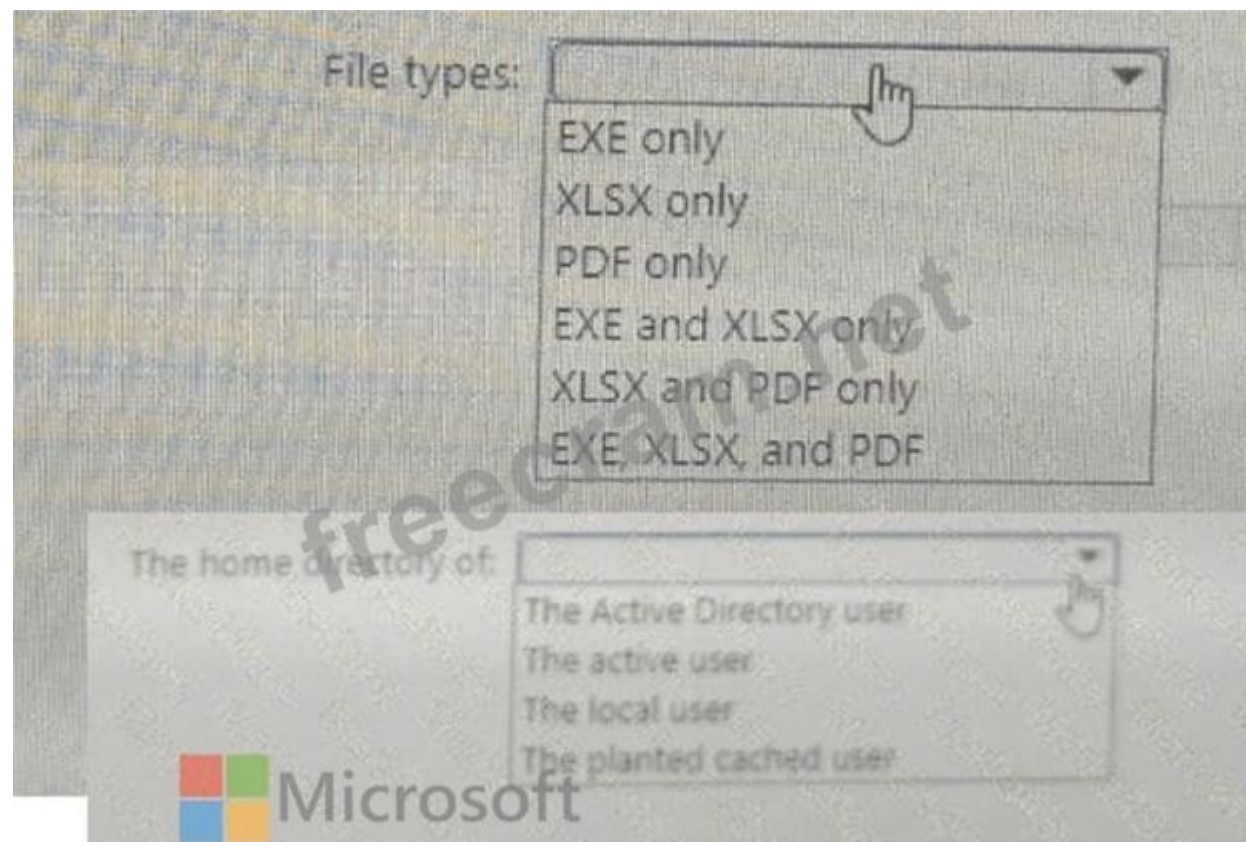
You are implementing a deception rule.

You need to provide a custom lure file.

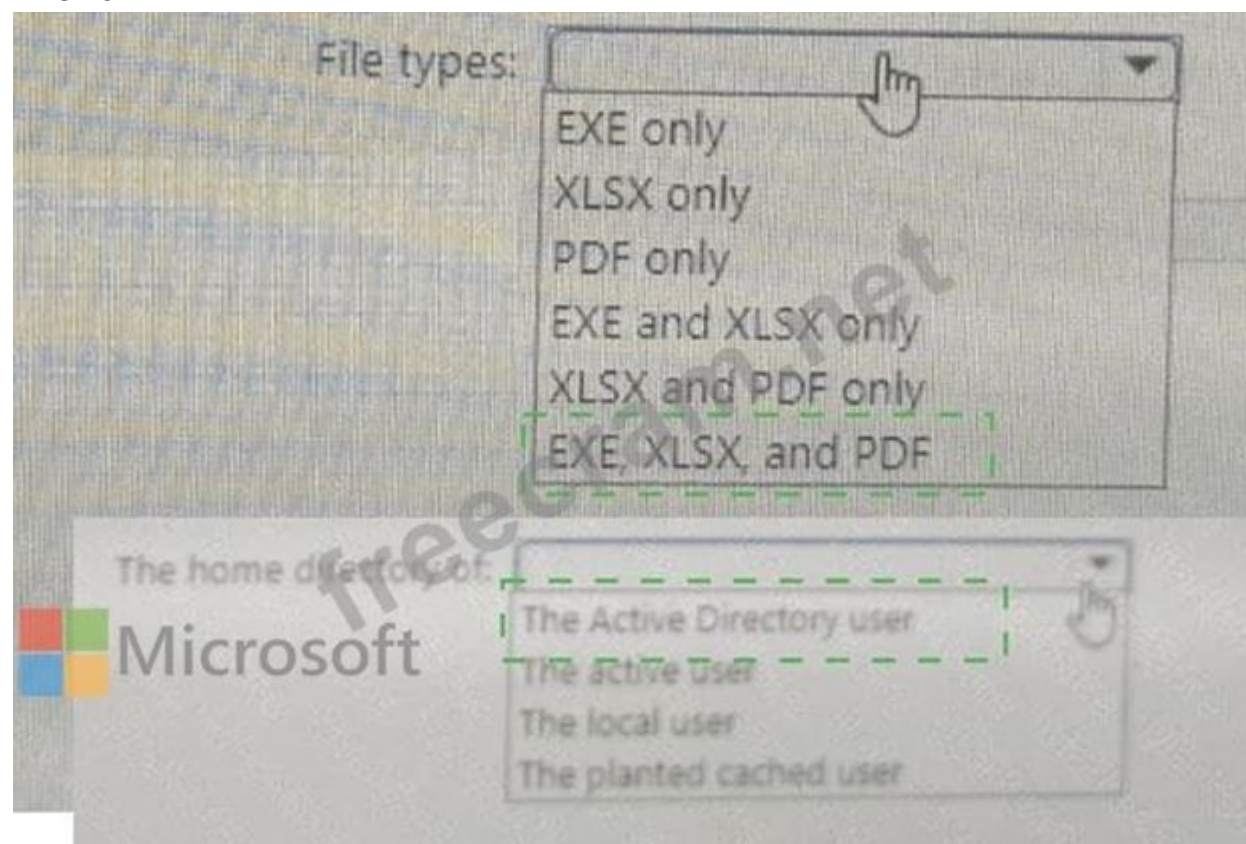
For the custom lure, you set Planting path to HOME.

Which types of files can you use for the custom lure, and in which home directory should the file be located on a device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



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?

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.

Question Part 2: In which home directory should the file be located on a device?

answer:

The Active Directory user

When you set the Planting path to HOME in a deception rule, the file should be planted in the home directory of a user. According to the available drop-down options and Microsoft documentation, the typical recommended choice for corporate environments (and specifically for most deception scenarios) is " The Active Directory user " . This ensures the lure is placed where the intended target (a domain user) is likely to encounter it.

NEW QUESTION: 118

You have a Microsoft Sentinel workspace that contains a custom workbook.

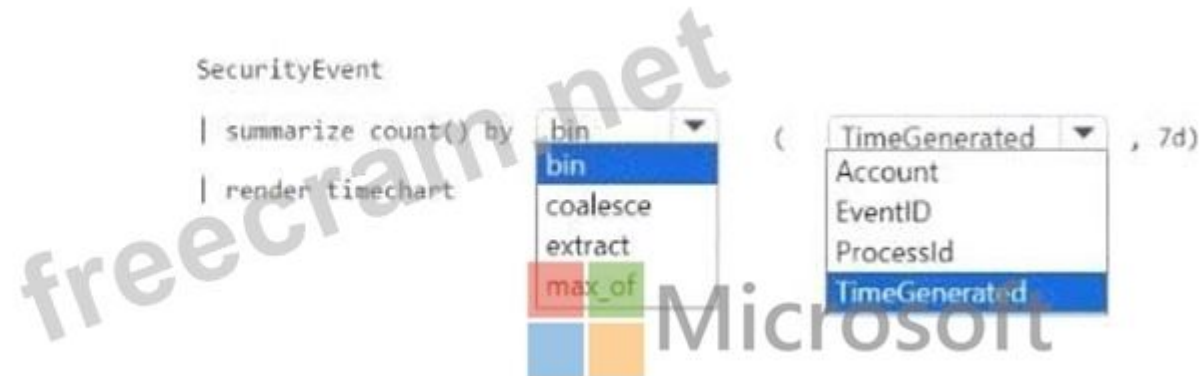
You need to query for a summary of security events. The solution must meet the following requirements:

- * Identify the number of security events ingested during the past week.
- * Display the count of events by day in a chart.

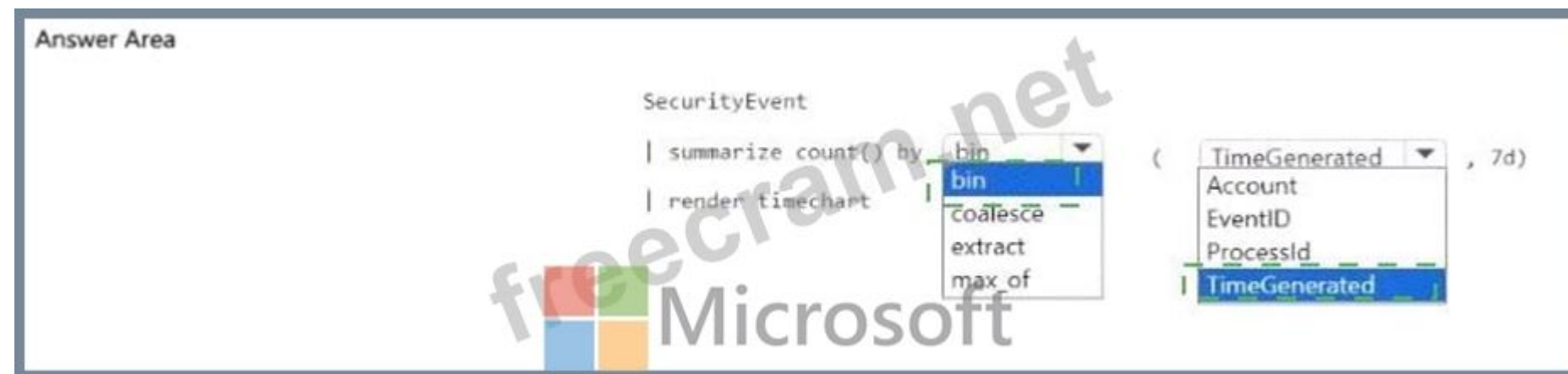
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



Explanation:



To summarize security events over the last week and chart them by day, use KQL time binning on the event timestamp. In Sentinel/Log Analytics, bin() groups records into fixed time buckets on a datetime column- here, TimeGenerated. Pair that with a time filter for the past 7 days and render as a timechart. The key pattern is:

SecurityEvent

| where TimeGenerated >= ago(7d)

| summarize Count = count() by bin(TimeGenerated, 1d)

| render timechart

* bin is the correct aggregator for time-based bucketing.

- * TimeGenerated is the standard timestamp column used across Sentinel tables for ingestion time.
- * Using a 1-day bin shows the daily counts; the where TimeGenerated > = ago(7d) limits results to the past week .
- * render timechart visualizes the grouped counts over time.

In the answer area shown, you select bin and TimeGenerated ; (the full query would also include the where line and a 1d bin size to meet the "by day" requirement).

NEW QUESTION: 119

You have an Azure subscription that contains 100 Linux virtual machines.

You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

Which three 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.

The screenshot shows the Microsoft Sentinel configuration interface. On the left, under the 'Actions' tab, there is a list of five actions: 'Add a Syslog connector to the workspace.', 'Add an Microsoft Sentinel workbook.', 'Add Microsoft Sentinel to a workspace.', 'Install the Log Analytics agent for Linux on the virtual machines.', and 'Add a Security Events connector to the workspace.'. On the right, there is an 'Answer Area' which is currently empty. Navigation arrows are visible on the right side of the interface.

Answer:

The screenshot shows the Microsoft Sentinel configuration interface with the correct sequence of actions moved to the 'Answer Area'. The actions are: 'Add Microsoft Sentinel to a workspace.', 'Install the Log Analytics agent for Linux on the virtual machines.', and 'Add a Security Events connector to the workspace.'. The 'Actions' list on the left remains the same. Navigation arrows are visible on the right side of the interface.

Explanation:

The screenshot shows the Microsoft Sentinel configuration interface with the correct sequence of actions in the 'Answer Area'. The actions are numbered 1, 2, and 3: 1. 'Add Microsoft Sentinel to a workspace.', 2. 'Install the Log Analytics agent for Linux on the virtual machines.', and 3. 'Add a Security Events connector to the workspace.'. The 'Actions' list on the left remains the same. Navigation arrows are visible on the right side of the interface.

To collect event logs from Linux virtual machines in Microsoft Sentinel, the data ingestion path must be correctly configured through Azure Monitor (Log Analytics) and Sentinel connectors . The correct order of actions is as follows:

1# # Add Microsoft Sentinel to a workspace:

Sentinel requires a Log Analytics workspace as its data foundation. You must first enable Microsoft Sentinel on a workspace by selecting Microsoft Sentinel # Add # Select workspace . This step prepares the workspace to receive and analyze security data.

2# # Add a Syslog connector to the workspace:

Linux systems send event data through Syslog . You must enable the Syslog connector within the Sentinel workspace. The connector defines which Syslog facilities and severities should be collected and ingested into Sentinel. It acts as the integration bridge between the Linux hosts and Sentinel's analytics engine.

3# # Install the Log Analytics agent for Linux on the virtual machines:

To forward the logs, each Linux virtual machine needs the Log Analytics agent (OMS agent) . This agent collects the configured Syslog and performance data and sends it to the connected Log Analytics workspace.

This sequence ensures proper setup for Linux log ingestion: Sentinel is first activated, then the Syslog data source is configured, and finally, agents are deployed to gather and transmit the logs.

NEW QUESTION: 120

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

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

NOTE: Each correct selection is worth one point.

MaliciousEmails

EmailAttachementInfo

EmailEvents

IdentityLogonEvents

where MalwareFilterVerdict == "Malware"

project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName

ostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails

join

EmailAttachementInfo

EmailEvents

IdentityLogonEvents

project LogonTime = Timestamp, AccountName, DeviceName

on AccountName

where (LogonTime - TimeEmail) between (0min.. 60min)

select 20

take 20

top 20

Answer:

```

let MaliciousEmails =
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
select 20
take 20
top 20

```

Explanation:

```

let MaliciousEmails =
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
select 20
take 20
top 20

```

Reference:

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

NEW QUESTION: 121

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.

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0
1
2
3

Query element required to correlate data between tenants:

extend
project
workspace

Answer:

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0
1
2
3

Query element required to correlate data between tenants:

extend
project
workspace

Explanation:

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

0
1
2
3

Query element required to correlate data between tenants:

extend
project
workspace

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: Fabrik am needs one workspace to host its Sentinel content, and you use workspace() in your KQL to correlate Contoso and Fabrikam data.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 122

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

- * The modification of local group memberships
- * The purging of event logs

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

Actions

From the details pane of the incident, select **Investigate**.

From the Investigation blade, select the entity that represents VM1.

From the Investigation blade, select the entity that represents powershell.exe.

From the Investigation blade, select **Timeline**.

From the Investigation blade, select **Info**.

From the Investigation blade, select **Insights**.

Answer Area

>

<

↑

↓

Answer:

The screenshot displays a Microsoft Azure Sentinel interface. On the left, under the heading 'Actions', there is a list of steps enclosed in dashed green boxes:

- From the details pane of the incident, select **Investigate**.
- From the Investigation blade, select the entity that represents VM1.
- From the Investigation blade, select the entity that represents powershell.exe.
- From the Investigation blade, select **Timeline**.
- From the Investigation blade, select **Info**.
- From the Investigation blade, select **Insights**.

On the right, under the heading 'Answer Area', there is a sequence of steps enclosed in dashed red boxes:

- From the Investigation blade, select **Insights**.
- From the Investigation blade, select the entity that represents VM1.
- From the details pane of the incident, select **Investigate**.

Arrows indicate the flow from the 'Actions' list to the 'Answer Area' steps. A large 'Microsoft' logo is visible in the background of the answer area.

Explanation:

Step 1: From the Investigation blade, select Insights

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

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

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

Incident Insights

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

Entity Insights

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

IP Address

Account

Host

URL

Step 3: From the details pane of the incident, select Investigate.

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

Reference:

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

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

NEW QUESTION: 123

You need to update the threat intelligence list to include the entities.

Which entities can you add on the Incident page?

A. 175.45.176.99 only

B. Host1 only

C. Used only

D. 175.45.176.99 and Host1 only

E. Host1 and User1 only

F. 175.45.176.99, Host1, and User1

Answer: ([SHOW ANSWER](#))

Threat intelligence indicator lists in Microsoft Defender support entities such as IP addresses, URLs/domains, and file hashes. Hosts (device names) and users are not valid TI indicator types to add from the Incident page.

Therefore, from the entities given, only the IP address 175.45.176.99 can be added to the threat intelligence list.

NEW QUESTION: 124

You have a Microsoft 365 E5 subscription.

Automated investigation and response (AIR) is enabled in Microsoft Defender for Office 365 and devices use full automation in Microsoft Defender for Endpoint.

You have an incident involving a user that received malware-infected email messages on a managed device.

Which action requires manual remediation of the incident?

- A. soft deleting the email message
- B. hard deleting the email message
- C. isolating the device
- D. containing the device

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 125

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Actions

Select Pricing & settings.

Select Security alerts.

Select IP as the entity type and specify the IP address.

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

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

Select Security policy.

Answer area



Answer:

Actions

Select **Pricing & settings**.

Select **Security alerts**.

Select **IP** as the entity type and specify the IP address.

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

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

Select **Security policy**.

Answer area

Select **Security policy**.

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

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

Explanation:



Reference:

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

NEW QUESTION: 126

You have an Azure subscription named Sub1. Sub1 contains a Microsoft Sentinel workspace named SW1 and a virtual machine named VM1 that runs Windows Server. SW1 collects security logs from VM1 by using the Windows Security Events via AMA connector.

You need to limit the scope of events collected from VM1. The solution must ensure that only audit failure events are collected.

How should you complete the filter expression for the connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Security!*[

System	EventData	Keywords	System[
	EventData	[Keywords='0x8010000000000000']	
	EventData		
	Keywords		
	System		

Microsoft

Answer:

Answer Area

Security!*[

System[
EventData[
Keywords[
System[

EventData[
EventData[
Keywords
System

[Keywords='0x8010000000000000']]

Microsoft

Explanation:

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

In Microsoft Sentinel, when using the Windows Security Events via AMA (Azure Monitor 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).

* Keywords= ' 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 ' ]]
```

NEW QUESTION: 127

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

- A. Azure Sentinel Contributor**
B. Security Administrator
C. Azure Sentinel Responder
D. Logic App Contributor

Answer: (SHOW ANSWER)

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>

NEW QUESTION: 128

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign- events in near real time.

What should you do to route events to the SIEM solution?

- A.** Create an Azure Sentinel workspace that has a Security Events connector.
- B.** Configure the Diagnostics settings in Azure AD to stream to an event hub.
- C.** Create an Azure Sentinel workspace that has an Azure Active Directory connector.
- D.** Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 129

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three 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.

Actions



Microsoft

Answer Area

From Device Inventory, search for the CVE.

Open the Threat Protection report.

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

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

Create the remediation request.

Select **Security recommendations**.



Answer:

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

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

From Advanced hunting, search for cveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

Create the remediation request.

Select **Security recommendations**.

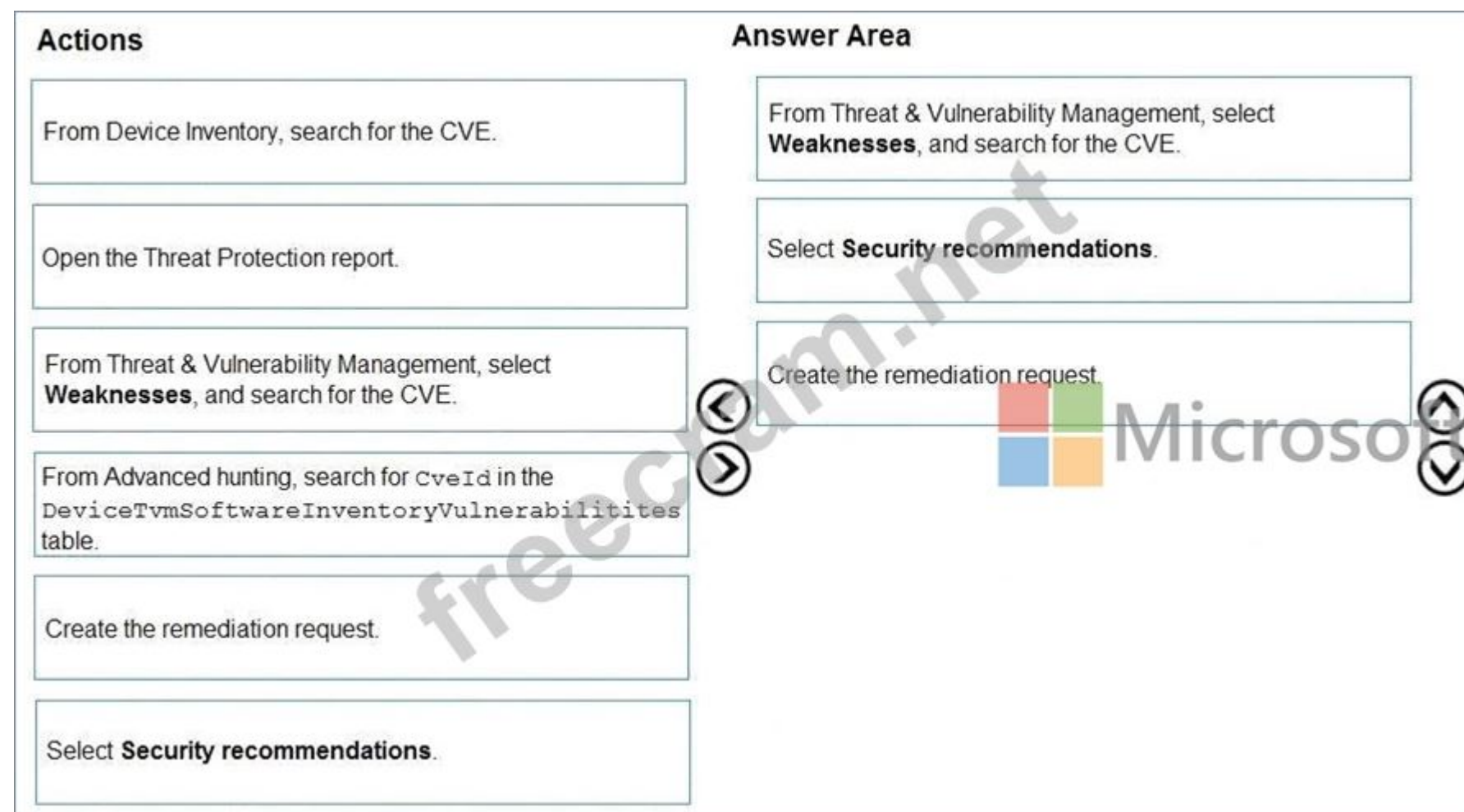
Answer Area

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

Select **Security recommendations**.

Create the remediation request.

Explanation:



According to official Microsoft Defender Vulnerability Management (TVM) documentation, when a new CVE is announced, analysts can use Microsoft 365 Defender Security Center to investigate exposure and initiate remediation workflows. The proper sequence to handle such a case is:

* From Threat & Vulnerability Management (TVM), select Weaknesses and search for the CVE. In Microsoft 365 Defender, all known vulnerabilities are cataloged under the Weaknesses tab. Searching for the CVE there allows security teams to determine whether any managed assets are affected and to view metadata such as severity, exploitability, and exposure score.

* Select Security recommendations. Once the CVE is located, associated Security recommendations appear. These recommendations include actionable steps like "Update software" or "Remove vulnerable version." Each recommendation aggregates affected devices, user exposure, and related CVEs.

* Create the remediation request. From the recommendation, analysts can create a remediation request directly in the Defender portal. This task is automatically assigned to the appropriate remediation group or IT operations team, with a due date and priority based on the risk assessment.

This workflow minimizes administrative effort, ensures alignment with the principle of least privilege, and leverages Defender's built-in Threat & Vulnerability Management (TVM) automation to move from detection to remediation efficiently.

Final Sequence:

(1) From Threat & Vulnerability Management # Weaknesses

(2) Select # Security recommendations

(3) Create # Remediation request

NEW QUESTION: 130

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains "" and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Block DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Answer: ([SHOW ANSWER](#))

In Microsoft 365 Defender advanced hunting, if you want to automatically receive alerts based on a KQL query-such as detecting when a process disables System Restore-you must convert that query into a custom detection rule . According to Microsoft's official documentation, custom detection rules "run hunting queries on a schedule and create alerts and incidents when results are found." In order for the detection rule to function properly and correlate results across devices and incidents, the query must output DeviceId and ReportId . These fields are mandatory for any advanced hunting query that you want to convert into a detection rule because they uniquely identify the device and event instance. Without them, the rule cannot properly generate correlated alerts.

Therefore:

- * Create a detection rule (A) - ensures the query runs automatically and alerts are generated.
- * Add DeviceId and ReportId (E) - required for detection rule creation and accurate device/event correlation.

Other options are incorrect:

- * Suppression rule (B) filters alerts, not generate them.
- * Order by Timestamp (C) is optional for display, not alerting.
- * DeviceNetworkEvents (D) is unrelated to this process query.

NEW QUESTION: 131

You have a Microsoft Sentinel workspace named Workspace1 that contains the AzureActivity table.

You need to configure the retention period for the AzureActivity table. The solution must meet the following requirements:

- * Maximize the period during which you can run interactive queries.
- * Minimize retention costs.

To what should you set the retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

- A. 2 years
- B. 90 days
- C. 180 days
- D. 30 days

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 132

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

Data source to query:

JSON

A custom endpoint

A custom resource provider

JSON

On Webapp1:

Enable Cross-Origin Resource Sharing (CORS).

Enable Cross-Origin Resource Sharing (CORS).

Enable Same Origin Policy (SOP).

Enforce TLS 1.2.

Answer:

Answer Area

Data source to query:

JSON

A custom endpoint

A custom resource provider

JSON

On Webapp1:

Enable Cross-Origin Resource Sharing (CORS).

Enable Cross-Origin Resource Sharing (CORS).

Enable Same Origin Policy (SOP).

Enforce TLS 1.2.

Explanation:

Answer Area

Data source to query:

JSON

On Webapp1:

Enable Cross-Origin Resource Sharing (CORS).

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.

NEW QUESTION: 133

You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

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

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Answer: ([SHOW ANSWER](#))

When creating analytics rules in Microsoft Sentinel (as shown in the rule query image), alerts can be grouped into incidents based on key entities. The extend command in the query defines custom entity map pings - in this case:

extend AccountCustomEntity = Account, HostCustomEntity = Computer

This configuration means Sentinel recognizes Account (User) and Computer (Host) as entities to correlate alerts. Incidents will group alerts sharing the same user account or computer , improving investigation efficiency.

According to Microsoft's incident grouping guidance:

"You can group alerts into incidents by entities such as Account, Host, IP, URL, or custom-defined entities in the query." Hence, the correct answers are A. User and D. Computer .

NEW QUESTION: 134

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

- A. a URL/domain indicator that has Action set to Alert only
- B. a URL/domain indicator that has Action set to Alert and block
- C. a file hash indicator that has Action set to Alert and block
- D. a certificate indicator that has Action set to Alert and block

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 135

You have a Microsoft 365 E5 subscription that contains a database server named DB1. DB1 is onboarded to Microsoft Defender XDR.

You need to ensure that DB1 appears on the attack surface map.

What should you configure?

A. a critical asset rule

B. an asset rule

C. a honeypot entity tag

D. a sensitive entity tag

Answer: ([SHOW ANSWER](#))

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 rules 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 configure 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.

* Honeypot 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

NEW QUESTION: 136

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

B. Create an Azure logic app that has a manual trigger

C. Create an Azure logic app that has an Azure Security Center alert trigger.

D. Create an Azure logic app that has an HTTP trigger.

E. From Azure Active Directory (Azure AD), add an app registration.

Answer: ([SHOW ANSWER](#))

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.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1. You need to ensure that the users can perform the following tasks in workspace1:

- * User1 must be able to dismiss incidents and assign incidents to users.
- * User2 must be able to modify analytics rules.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

Contributor

Microsoft Sentinel Automation Contributor

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

Reader

Answer Area

User1:

User2:

Answer:

Roles

Contributor

Microsoft Sentinel Automation Contributor

Microsoft Sentinel Contributor

Microsoft Sentinel Reader

Microsoft Sentinel Responder

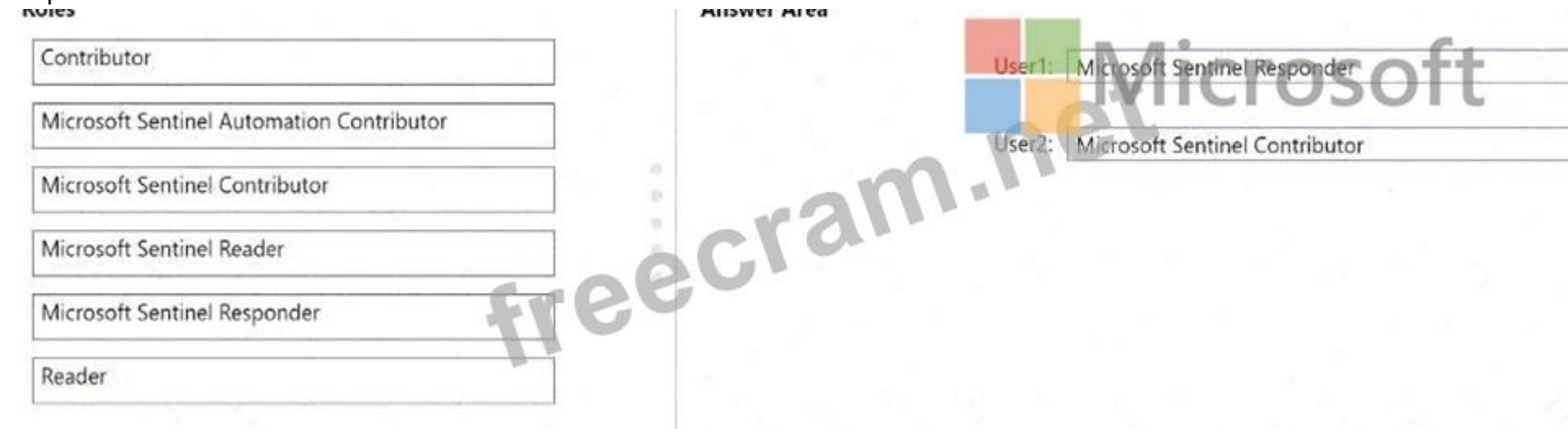
Reader

Answer Area

User1: Microsoft Sentinel Responder

User2: Microsoft Sentinel Contributor

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 handling 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 requirements 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 Reader: View-only permissions.

- * Microsoft Sentinel Automation Contributor: Allows playbook and automation editing.

- * Contributor/Reader: General Azure roles, not Sentinel-specific.

NEW QUESTION: 138

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi-factor authentication (MFA).

You need to enforce MFA for all users who work remotely.

What should you include in the solution?

A. a fraud alert

B. a user risk policy

C. a named location

D. a sign-in user policy

Answer: ([**SHOW ANSWER**](#)**)**

To enforce Multi-Factor Authentication (MFA) for remote users, Microsoft recommends using Conditional Access policies that distinguish between trusted (corporate) and untrusted (remote) network locations.

In Azure AD Conditional Access, this is implemented using Named Locations. You define a named location by specifying trusted IP address ranges for your corporate network. The policy can then enforce MFA for sign- ins that originate outside those trusted locations.

Microsoft Learn states:

"Use named locations in Conditional Access to define network boundaries for your organization and configure policies to enforce MFA for users accessing from untrusted networks."

Correct answer: C. a named location

NEW QUESTION: 139

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachment s take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A.** Dynamic Delivery
- B.** Replace
- C.** Block and Enable redirect
- D.** Monitor and Enable redirect

Answer: ([**SHOW ANSWER**](#)**)**

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

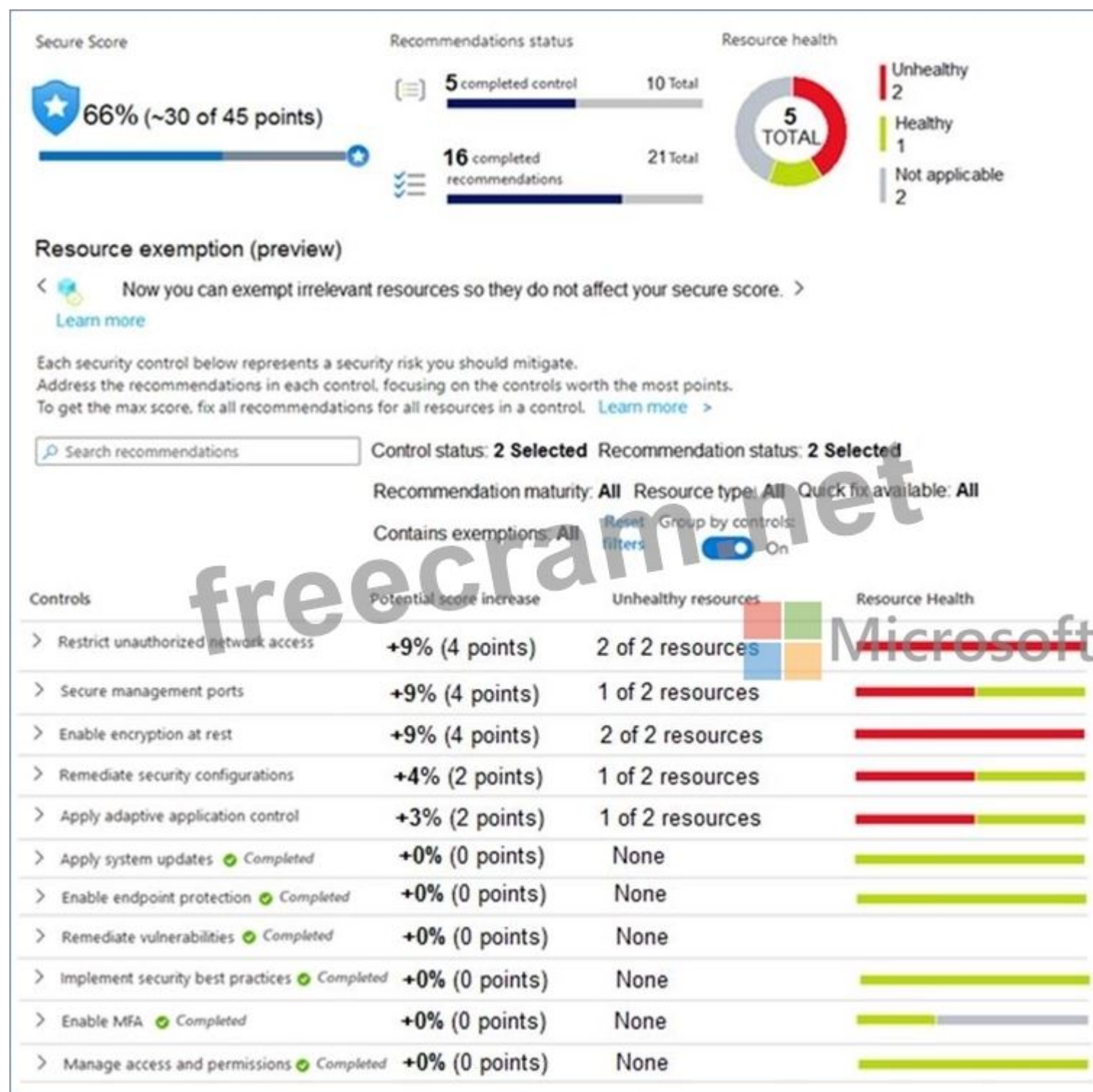
. If malware is found, the attachment is blocked/removed and the message is handled per policy (for example, quarantined) . This option meets both requirements in the question: (1) users get messages quickly (no long wait for full message delivery) and (2) security isn't reduced because attachments are 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.

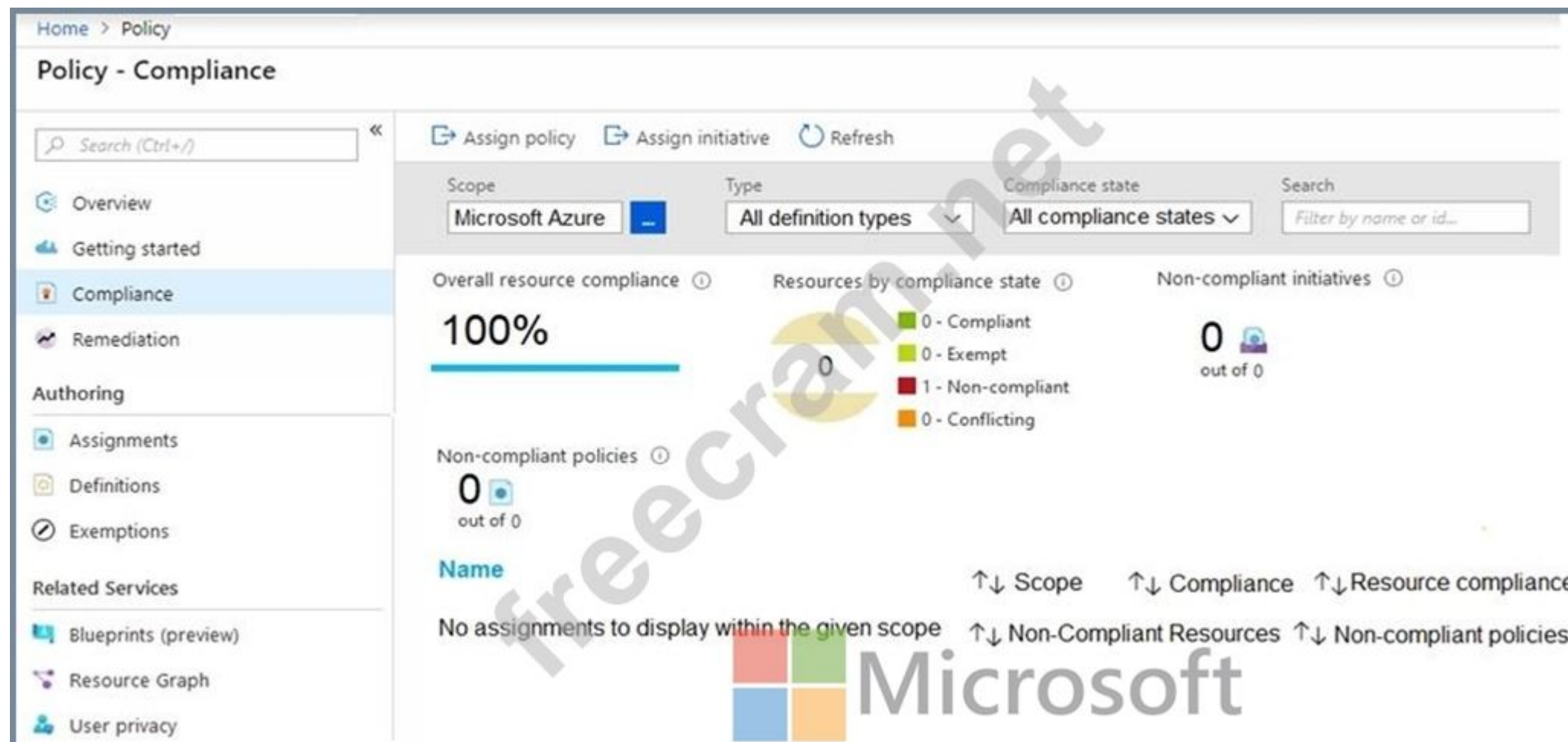
NEW QUESTION: 140

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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 points.

☐
☐

Answer:

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 points.	☐	☐

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 controls 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 (JIT) 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 "Potential 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 override. 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 .

NEW QUESTION: 141

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 142

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

- A.** the risk detections report
- B.** the risky users report
- C.** Identity Secure Score recommendations
- D.** the risky sign-ins report

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 143

You have a Microsoft Sentinel workspace.

You need to configure a report visual for a custom workbook. The solution must meet the following requirements:

- * The count and usage trend of AppDisplayName must be included
- * The TrendList column must be useable in a sparkline visual,

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

NOTE: Each correct selection is worth one point.

Answer Area

SignInLogs

```
| where ResultType == 0 and AppDisplayName != ""
```

```
| summarize count() by AppDisplayName
```

```
| join (
```

```
SignInLogs
```

```
| let
```

```
| lookup
```

```
| mv-expand
```

```
) on AppDisplayName
```

```
| top 10 by count_desc
```

SignInLogs

```
| make-series
```

```
make_bag()
```

```
make-series
```

```
mv-expand
```

```
render
```

```
) on AppDisplayName
```

```
| top 10 by count_desc
```

TrendList = count() on TimeGenerated in range([TimeRange:start], [TimeRange:end], 4h) by AppDisplayName

TrendList = count() on TimeGenerated in range([TimeRange:start], [TimeRange:end], 4h) by AppDisplayName



Answer:

Answer Area



SigninLogs

```
| where ResultType == 0 and AppDisplayName != ""
```

```
| summarize count() by AppDisplayName
```

```
| join (
```

```
| join
```

```
| let
```

```
| lookup
```

```
| mv-expand
```

```
) on AppDisplayName
```

TrendList = count() on TimeGenerated in range([TimeRange:start], [TimeRange:end], 4h) by AppDisplayName

```
| top 10 by count_desc
```

SigninLogs

```
| make-series
```

TrendList = count() on TimeGenerated in range([TimeRange:start], [TimeRange:end], 4h) by AppDisplayName

```
| make_bag()
```

```
| make-series
```

```
| mv-expand
```

```
| render
```

```
) on AppDisplayName
```

```
| top 10 by count_desc
```

Explanation:

Answer Area

SigninLogs

```
| where ResultType == 0 and AppDisplayName != ""
```

```
| summarize count() by AppDisplayName
```

```
| join (
```

SigninLogs

```
| make-series
```

TrendList = count() on TimeGenerated in range([TimeRange:start], [TimeRange:end], 4h) by AppDisplayName

```
) on AppDisplayName
```

```
| top 10 by count_desc
```



NEW QUESTION: 144

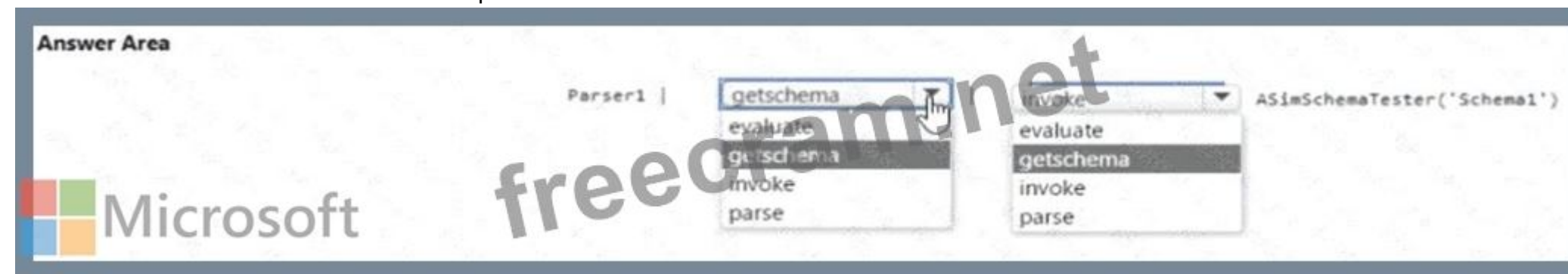
You have a Microsoft Sentinel workspace

You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

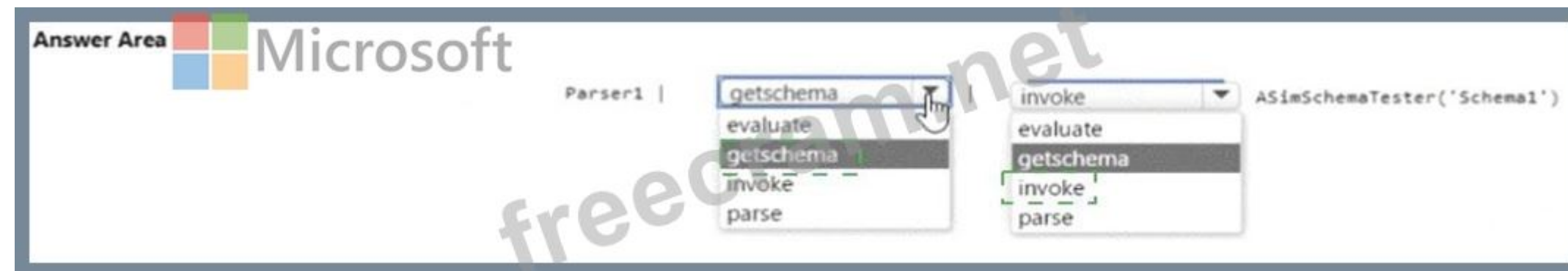
You need to validate Schema1.

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

NOTE: Each correct selection is worth one point.



Answer:



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 getschema 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 ') .

NEW QUESTION: 145

You have 1,000 on-premises Windows 11 Pro devices that are onboarded to Microsoft Defender for Endpoint.

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. You identify that an attacker performed the following actions on a device:

- * Modified the file system path of a registry-based antivirus exclusion
- * Downloaded a malicious file to the file system path

You initiate a live response session on the device. You need to undo the registry change. Which command should you run?

A. analyze

- B. registry
- C. remediate
- D. scan

Answer: (SHOW ANSWER)

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 attacker 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.

- * analyze 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

NEW QUESTION: 146

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1. WS1 uses Microsoft Defender for Cloud.

You have the Microsoft security analytics rules shown in the following table.

Name	Service	Severity	Action
Rule1	Defender for Cloud	High	Create incident
Rule2	Defender for Cloud	High	Create incident
Rule3	Defender for Cloud	High	Create incident
Rule4	Defender for Cloud	High	Create incident

User1 performs an action that matches Rule1, Rule2, Rule3, and Rule4. How many incidents will be created in WS1?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: (SHOW ANSWER)

Microsoft Sentinel "Microsoft security" analytics rules (for products like Defender for Cloud) create incidents from alerts generated by that product. Even if multiple identical Microsoft security rules exist for the same product, a single incoming alert will result in one incident in the workspace, not one per rule.

NEW QUESTION: 147

You have the resources shown in the following table.

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

You need to prevent duplicate events from occurring in SW1.

What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Resources

**Answer Area**

SW1	From the Syslog configuration, remove the facilities that send CEF messages.	
CEF1		
Server1	From the Log Analytics agent, disable Syslog synchronization.	
Server2		

Answer:

Resources

**Answer Area**

SW1	From the Syslog configuration, remove the facilities that send CEF messages.	CEF1
CEF1		
Server1	From the Log Analytics agent, disable Syslog synchronization.	Server2
Server2		

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

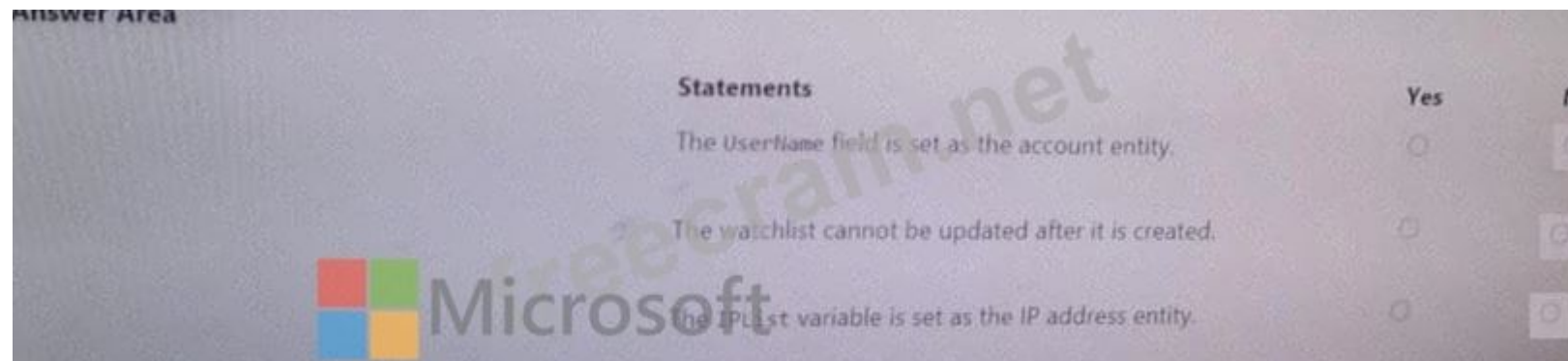
* According to Microsoft Sentinel documentation on log ingestion, when using a dedicated forwarder (like CEF1) for Syslog/CEF, you must disable the Syslog collection on the Log Analytics agent of the source machine (Server2) to prevent this duplication. This is typically done by disabling Syslog synchronization 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.

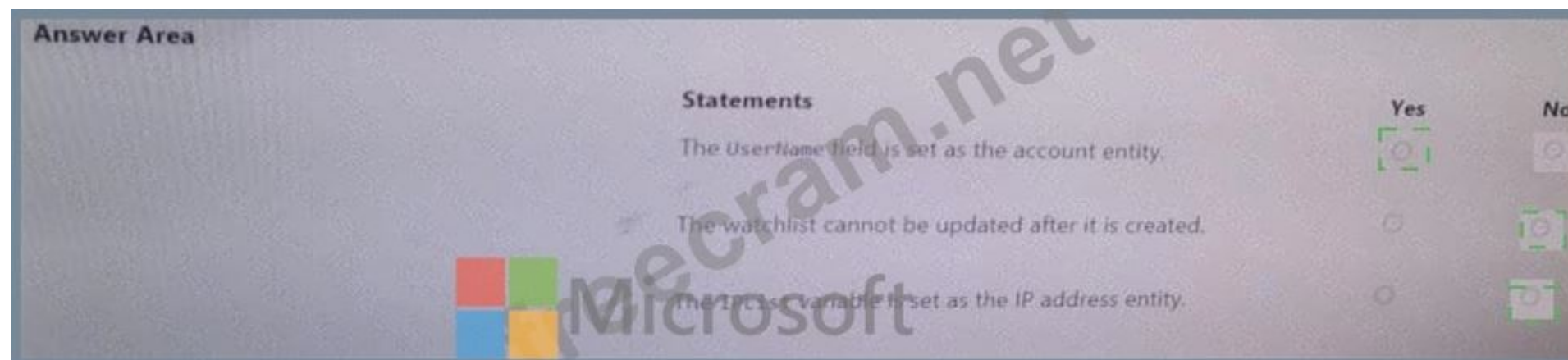
NEW QUESTION: 148

You have the following SQL query.

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



Answer:



Explanation:

The Username field is set as the account entity. # Yes

The watchlist cannot be updated after it is created. # No

The IPList variable is set as the IP address entity. # No

In Microsoft Sentinel analytics rules, entity mapping is done by assigning special alias fields in the query result such as AccountCustomEntity , HostCustomEntity , and IPCustomEntity . In the provided KQL, the final line explicitly maps AccountCustomEntity = Username and HostCustomEntity = Computer , which sets Username as the account entity and Computer as the host entity. No mapping is provided for an IP entity; the query defines let IPList = _GetWatchlist(' Bad_IPs '); to retrieve a watchlist named Bad_IPs and then uses it only for filtering (SourceIP in (IPList) or DestinationIP in (IPList)). Because IPList is a dataset used for comparison and not assigned to IPCustomEntity , it is not set as the IP address entity. Additionally, Microsoft Sentinel watchlists are editable -you can upload new files, append, or replace data after creation-so the statement that a watchlist cannot be updated is false .

NEW QUESTION: 149

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

In the identity environment, implement:

- Azure AD Password Protection
- Azure AD Password Protection
- Microsoft Defender for Identity
- Smart lockout

In Microsoft Sentinel, configure:

- The Windows Security Events via AMA connector
- A Microsoft security rule
- The Windows Security Events via AMA connector
- User and Entity Behavior Analytics (UEBA)

Explanation:

Answer Area

In the identity environment, implement: Azure AD Password Protection

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

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

NEW QUESTION: 150

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. As part of an incident investigation, you identify the following suspected malware files:

- * sys
- * pdf
- * docx
- * xlsx

You need to create indicator hashes to block users from downloading the files to the devices. Which files can you block by using the indicator hashes?

- A. File1.sysonly
- B. File1.sysand File3.docxonly
- C. File1.sys, File3.docx, and File4jclsx only
- D. File2.pdf, File3.docxr and File4.xlsx only
- E. File1.sys, File2.pdf, File3.dooc, and File4.xlsx

Answer: ([SHOW ANSWER](#))

In Microsoft Defender for Endpoint (Plan 2), you can use indicator file hashes (IoC file hashes) to block files from 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. Because 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 can 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 Microsoft'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.

NEW QUESTION: 151

You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	



Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Answer:

Microsoft Teams:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Custom</td></tr><tr><td colspan="2">Office 365</td></tr><tr><td colspan="2">Security Events</td></tr><tr><td colspan="2">Syslog</td></tr></table>		▼	Custom		Office 365		Security Events		Syslog	
	▼										
Custom											
Office 365											
Security Events											
Syslog											
Linux virtual machines in Azure:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Custom</td></tr><tr><td colspan="2">Office 365</td></tr><tr><td colspan="2">Security Events</td></tr><tr><td colspan="2">Syslog</td></tr></table>		▼	Custom		Office 365		Security Events		Syslog	
	▼										
Custom											
Office 365											
Security Events											
Syslog											

Explanation:



	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

In Microsoft Sentinel (part of Microsoft Defender XDR), data connectors are used to integrate log sources for security analytics and monitoring.

For Microsoft Teams , the correct and most efficient connector is Office 365 . Microsoft Teams logs- including user activities, chat events, and team management actions-are part of the Office 365 audit logs .

Microsoft Sentinel provides a built-in Office 365 connector that ingests auditing data from Exchange Online, SharePoint Online, and Microsoft Teams directly from the Microsoft 365 security and compliance center.

This connector requires only minimal configuration (enabling audit logging and connecting the tenant), satisfying the requirement to minimize administrative effort .

For Linux virtual machines hosted in Azure , the appropriate connector is Syslog . Linux systems send their security and operational events via Syslog, and Microsoft Sentinel supports this natively through the Syslog data connector . The Syslog agent (Log Analytics agent or AMA) collects logs and sends them to the Sentinel workspace. This connector is purpose-built for Linux VMs and ensures that authentication, authorization, and system logs are captured for correlation and threat detection.

Therefore:

* Microsoft Teams # Office 365 (because Teams audit data flows via Office 365 logs)

* Linux virtual machines in Azure # Syslog (because Linux uses Syslog for event forwarding) This configuration follows Microsoft's documented best practices for Sentinel data ingestion with minimal setup and maximum native integration.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (415 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 152

You have a Microsoft Sentinel workspace named SW1.

In SW1. you enable User and Entity Behavior Analytics (UEBA).

You need to use KQL to perform the following tasks:

- * View the entity data that has fields for each type of entity.
- * Assess the quality of rules by analyzing how well a rule performs.

Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks.

Each table may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Tables

Anomalies

AuditLogs

AzureDiagnostics

BehaviorAnalytics

CommonSecurityLog

Answer Area

View entity data:

Assess rule quality:

Answer:

Tables

Anomalies

AuditLogs

AzureDiagnostics

BehaviorAnalytics

CommonSecurityLog

Answer Area

View entity data: BehaviorAnalytics

Assess rule quality: Anomalies

Explanation:

Tables

Anomalies

AuditLogs

AzureDiagnostics

BehaviorAnalytics

CommonSecurityLog

Answer Area

View entity data: BehaviorAnalytics

Assess rule quality: Anomalies

When User and Entity Behavior Analytics (UEBA) is enabled in Microsoft Sentinel , it creates several dedicated tables within the Log Analytics workspace to store pr ocessed data for behavioral analytics and anomaly detection. Each table serves a specific purpose according to Microsoft documentation.

* BehaviorAnalytics Table - for viewing entity data The BehaviorAnalytics table stores enriched information about entities (such as users, hosts, IP addresses, and applications) and their observed behaviors. Each record includes multiple fields that describe user or entity activities, risk scores, and behavioral baselines. Microsoft Sentinel documentation states:

"Use the BehaviorAnalytics table to view the entity data collected and analyzed by UEBA. This table contains fields for each type of entity, including account, host, and IP data." Therefore, to view the entity data with detailed attributes for each type, you query the BehaviorAnalytics table in KQL.

* Anomalies Table - for assessing rule quality The Anomalies table is used to analyze the results of anomaly detection rules and evaluate their effectiveness. Each record represents an anomaly event generated by UEBA's machine learning or statistical models. Microsoft's UEBA and Sentinel analytics documentation explains:

"Use the Anomalies table to assess the performance and quality of your anomaly detection rules. The table helps you identify how well each rule detects unusual activities and whether it produces false positives." Thus, when you need to measure how well your rules perform (i.e., their quality, hit rate, or alert effectiveness), you use the Anomalies table.

Summary Mapping:

* View entity data # BehaviorAnalytics

* Assess rule quality # Anomalies

This mapping aligns directly with the functionality of UEBA-related tables in Microsoft Sentinel and follows official documentation for analyzing entity behaviors and anomaly rule performance.

NEW QUESTION: 153

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: ([SHOW ANSWER](#))

When dealing with frequent false positives in Microsoft Defender for Endpoint alerts, such as those triggered by legitimate Office macros, the best practice is to hide false alerts while maintaining overall protection.

Microsoft Defender documentation prescribes the following approach:

- * Generate the alert (E): The alert must first appear in the queue so it can be reviewed and correctly classified.
- * Hide the alert (B): Analysts can hide individual alerts to clean up the queue without disabling detections or reducing coverage.
- * Create a suppression rule scoped to a device group (D): To prevent recurrence, suppression rules should be scoped narrowly (such as to a device group like the accounting team's devices), maintaining the principle of least privilege and minimal impact.

Options A (Resolve automatically) and C (Suppress any device) would reduce visibility or broaden suppression excessively, potentially missing real threats.

This combination of actions aligns with Defender XDR's alert management best practices, ensuring a balance between reducing noise and preserving security posture.

NEW QUESTION: 154

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
- C. Select Add indicator and set the IP address to 171.23.34.32/27
- D. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.

Answer: D ([LEAVE A REPLY](#))

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference: [1] <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence-manage-indicators>

NEW QUESTION: 155

You have an Azure subscription named Sub1 and an Azure DevOps organization named AzDO1. AzDO1 uses Defender for Cloud and contains a project that has a YAML pipeline named Pipeline1. Pipeline1 outputs the details of discovered open source software vulnerabilities to Defender for Cloud.

You need to configure Pipeline1 to output the results of secret scanning to Defender for Cloud. What should you add to Pipeline1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 156

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.

You are troubleshooting an issue on the virtual machines.

In Security Center, you need to view the alerts generated by the virtual machines during the last five days.

What should you do?

- A. Change the rule expiration date of the suppression rule.
- B. Change the state of the suppression rule to Disabled.
- C. Modify the filter for the Security alerts page.

D. View the Windows event logs on the virtual machines.

Answer: (SHOW ANSWER)

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.

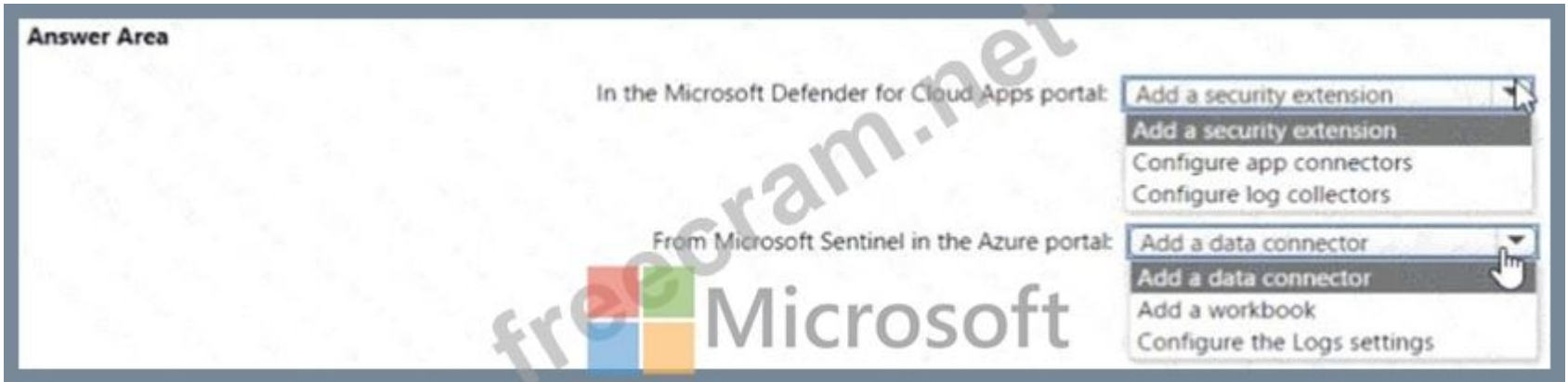
Modifying filters (Option C) won't reveal suppressed alerts, as those are already hidden from query results.

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.

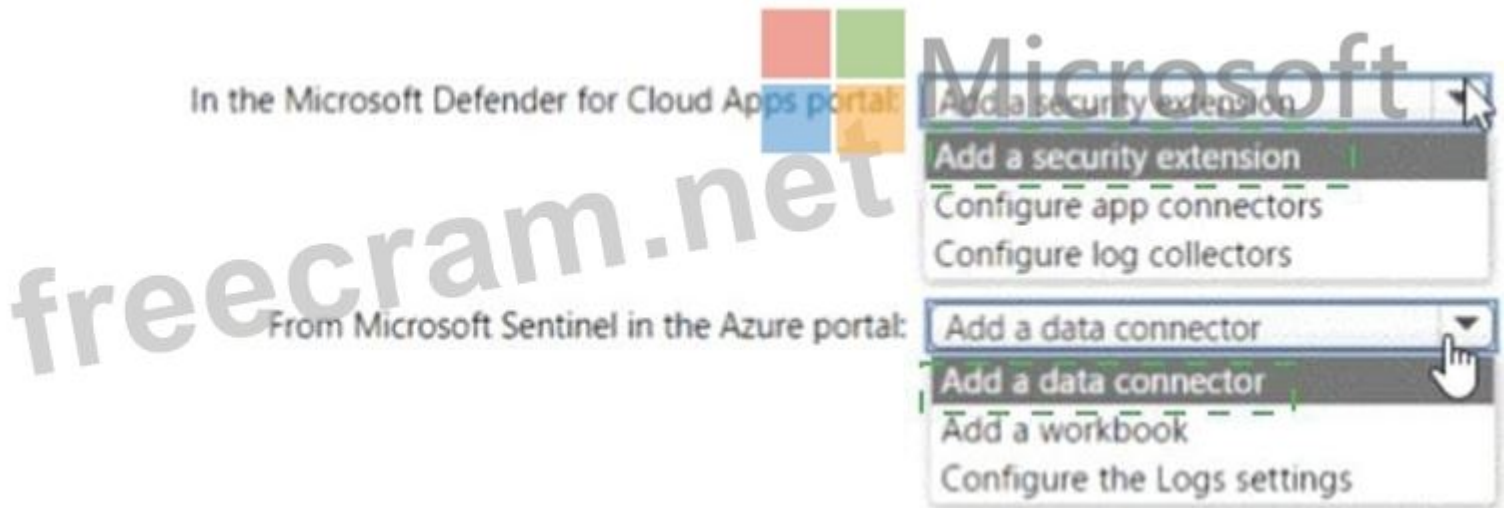
NEW QUESTION: 157

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:

Answer Area



Explanation:

Answer Area



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

NEW QUESTION: 158

You have a Microsoft Sentinel workspace named sws1.

You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.

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

```

| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
  BehaviorAnalytics
  AuditLogs
  AzureActivity
  BehaviorAnalytics
  SecurityEvent
  | where ActivityInsights.AccountDisplayName == $right._ItemId
  | sort by TimeGenerated desc
  | project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
  ActivityType, ActionType

```

Answer:

Answer Area

```
AzureActivity
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

| where ActionType == "Add user"

| where ActivityInsights has "True"

| join(

BehaviorAnalytics
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

= $right._ItemId

covering(UsersInsights.AccountDisplayName),

| sort by TimeGenerated desc

| project TimeGenerated, Username, UserPrincipalName, UsersInsights,
ActivityType, ActionType
```

Explanation:

First table: BehaviorAnalytics

Joined table: AuditLogs

To detect when a user creates an unusually large number of Azure AD user accounts in Microsoft Sentinel, 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 normalized 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 outliers.

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 and 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(...) .

NEW QUESTION: 159

You have an Azure subscription that has the enhanced security features in Microsoft Defender for Cloud enabled and contains a user named User1.

You need to ensure that User1 can export alert data from Defender for Cloud. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Contributor

- B. User Access Administrator
- C. Owner
- D. Reader

Answer: ([SHOW ANSWER](#))

In Microsoft Defender for Cloud, exporting alert data (for example, to Event Hubs, Log Analytics, or external SIEM tools like Microsoft Sentinel) does not require modification of resources or configurations- only read access to security data.

According to Microsoft's official documentation, the "Reader" role provides view-only access to all Defender for Cloud data, including security alerts, recommendations, regulatory compliance, and inventory.

This role allows users to export alert data, use APIs, and view findings, without granting permissions to make changes in the Defender for Cloud configuration.

Other roles explained:

- * Owner - Full access to all resources, including assigning roles (too high privilege).
 - * Contributor - Can make configuration changes, such as enabling plans or modifying policies (unnecessary for exporting).
 - * User Access Administrator - Manages role assignments only, not security data.
- # Therefore, the Reader role follows the principle of least privilege and allows exporting Defender for Cloud alert data.

NEW QUESTION: 160

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.

What should you configure first?

- A. the Azure connector
- B. the User enrichment settings
- C. the Automatic log upload settings
- D. the Microsoft 365 connector

Answer: ([SHOW ANSWER](#))

To investigate threats using data from the unified audit log in Microsoft Defender for Cloud Apps, you must 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 for 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 from 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 .

NEW QUESTION: 161

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You need to create a custom detection rule that will identify devices that had more than five antivirus detections within the last 24 hours.

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

```
DeviceEvents
| where ingestion_time() > ago(1d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, DeviceId) = arg_max(Timestamp, DeviceId), count() by DeviceId
| where count_ > 5
```

DeviceId

DeviceId
InitiatingProcessAccountObjectId
ReportId
TimeGenerated

DeviceId

DeviceId
InitiatingProcessAccountObjectId
ReportId
TimeGenerated

Answer:

Answer Area

```
DeviceEvents
| where ingestion_time() > ago(1d)
| where ActionType == "AntivirusDetection"
| summarize (Timestamp, DeviceId) = arg_max(Timestamp, DeviceId), count() by DeviceId
| where count_ > 5
```

DeviceId

DeviceId
InitiatingProcessAccountObjectId
ReportId
TimeGenerated

DeviceId

DeviceId
InitiatingProcessAccountObjectId
ReportId
TimeGenerated

Explanation:

First selection: ReportId

Second selection: ReportId

In Microsoft Defender XDR advanced hunting, antivirus detections on endpoints are recorded in DeviceEvents with ActionType == "AntivirusDetection". To find devices with more than five detections in the last 24 hours, filter the table to the last day, then summarize counts by DeviceId. To avoid returning multiple rows per device and to include a representative "latest" event field, use arg_max(Timestamp, ReportId) within summarize. The arg_max aggregation returns the row associated with the maximum Timestamp per device and keeps the ReportId from that latest event. Because you're projecting specific fields from arg_max, you must specify the same fields on both sides of the assignment: (Timestamp, ReportId) = arg_max(Timestamp, ReportId).

Final query pattern:

DeviceEvents

| where ingestion_time() > ago(1d)

| where ActionType == "AntivirusDetection"

| summarize (Timestamp, ReportId) = arg_max(Timestamp, ReportId), count() by DeviceId

| where count_ > 5

* ingestion_time() > ago(1d) ensures the last 24 hours relative to ingestion, aligning with fast, reliable time filtering.

* count() tallies detections per device; where count_ > 5 filters to devices exceeding the threshold.

* arg_max(Timestamp, ReportId) picks the latest detection per device and carries along a concrete identifier (ReportId) from that event.

NEW QUESTION: 162

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.** Enable Entity behavior analytics.
- B.** Associate a playbook to the analytics rule that triggered the incident.
- C.** Enable the Fusion rule.
- D.** Add a playbook.
- E.** Create a workbook.

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 163

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product.

Solution: You configure endpoint detection and response (EDR) in block mode.

Does this meet the goal?

- A.** Yes
- B.** No

Answer: ([SHOW ANSWER](#))

EDR in block mode is a Defender for Endpoint capability designed specifically for environments where a non-Microsoft antivirus is the primary real-time protection (i.e., Microsoft Defender Antivirus is running in passive mode). The official documentation explains that EDR in block mode "provides added protection from malicious artifacts when Microsoft Defender Antivirus is not the primary antivirus product." Practically, that means behavioral detections and EDR cloud signals can trigger remediation actions (quarantine, remove, kill process, etc.) even if the third-party AV missed the artifact. Microsoft explicitly states EDR in block mode remediates post-breach artifacts that were missed by the primary antivirus and is recommended for this scenario. Note that some prevention features that require Defender Antivirus active (on-access real-time scanning, certain ASR/network protection features) won't be available while Defender AV is passive, but EDR in block mode still provides post-detection blocking/remediation - which meets the stated goal of protecting devices from artifacts undetected by the third-party AV.

NEW QUESTION: 164

You open the Cloud App Security portal as shown in the following exhibit.

Cloud Discovery – Cloud App Security

https://m365x631117.portal.cloudappsecurity.com/#/discover?score=eq(0,3)&streamid=5e9f62ff2be23b5fd8b74d6a&tab=services

Cloud App Security

Cloud Discovery

Dashboard Discovered apps IP addresses Users

Queries

APPS APP TAG RISK SCORE Save as Advanced

COMPLIANCE RISK FACTOR SECURITY RISK FACTOR

Search by category

Cloud storage 5

Hosting services 3

IT services 3

Content management 3

Data analytics 2

Website monitoring 2

Advertising 2

Marketing 2

Customer support 2

Collaboration 2

App Score Traffic Upload Transac... Users IP addr... Last se... Actions

Applied Innovations Hosting services 866 KB - 12 11 8 Apr 20...

StatusCake Website monitoring 939 KB - 13 13 7 Apr 20...

Usersnap Productivity 1 MB - 15 15 10 Apr 20...

CopperEgg Website monitoring 866 KB - 12 12 8 Apr 20...

Launchpad Code-hosting 939 KB - 13 13 7 Apr 20...

You need to remediate the risk for the Launchpad app.

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.

Actions

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.

Answer Area

←

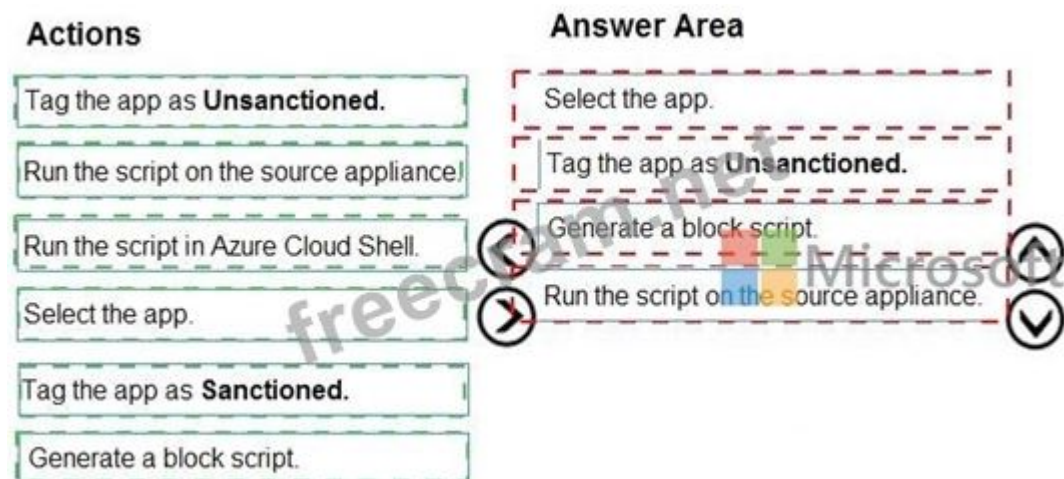
→

↑

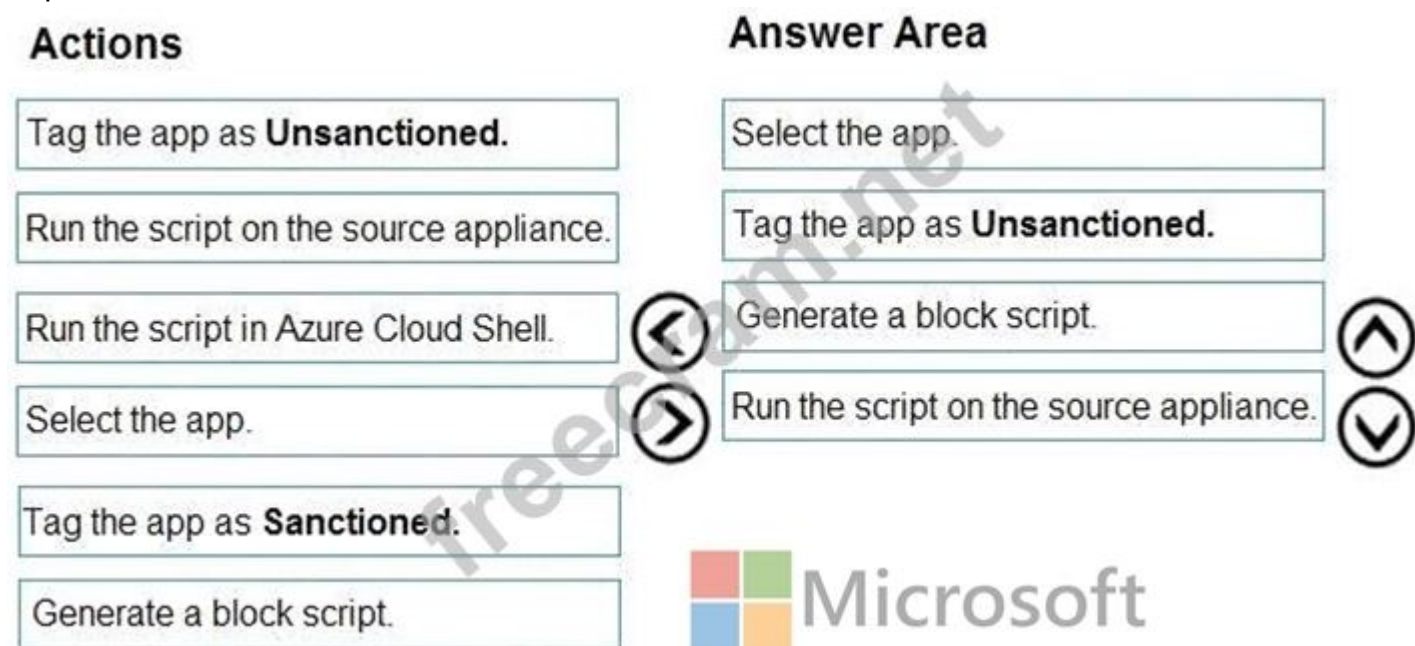
↓

Microsoft

Answer:



Explanation:



According to Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) documentation, when an application discovered by Cloud Discovery is deemed risky or non-compliant, the recommended remediation process is to unsanction it and enforce blocking through your network security devices or firewalls.

The process follows these four exact steps:

- * Select the app - In the Discovered apps tab, security analysts must first locate and select the risky application (in this case, Launchpad). Microsoft documentation states: "Select the discovered app that you want to remediate to open available actions."
- * Tag the app as Unsanctioned - Marking an app as Unsanctioned flags it as not allowed for organizational use. This designation helps track and automatically block or monitor it through connected security controls. Reference guidance: "Unsanction apps that you want to block across your network to prevent user access."
- * Generate a block script - Once an app is tagged as Unsanctioned , you can generate a block script compatible with your firewall or proxy device (such as Palo Alto, Cisco ASA, or Zscaler). Microsoft documentation explains: "From the unsanctioned app menu, select Generate block script to create a script for your appliance type."
- * Run the script on the source appliance - Finally, to enforce blocking, the generated script must be executed on the network appliance or proxy device that is integrated with Cloud Discovery. Official description: "Run the generated script on your network appliance to block unsanctioned apps." This sequence ensures compliance and reduces data exposure by automatically restricting high-risk apps, aligning with Microsoft SecOps best practices of proactive risk mitigation and least privilege.

Final Correct Order:

1. Select the app # 2. Tag the app as Unsanctioned # 3. Generate a block script # 4. Run the script on the source appliance

NEW QUESTION: 165

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode. You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product Solution: You enable automated investigation and response (AIR).

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 166

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Explanation (concise): The Regulatory compliance dashboard/report shows standards-based compliance posture and related recommendations across resources, not the alert-specific remediation steps. To view how to fix a specific Security Center (Defender for Cloud) alert, you open the alert, choose Take action, and review the Mitigate the threat guidance. Therefore, downloading the Regulatory compliance report does not meet the goal.

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (**415 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 167

You have a Microsoft 365 subscription that uses Microsoft Defender XDR and Microsoft Defender for Endpoint. The subscription contains the devices shown in the following table.

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

You discover the following forensic data:

- * During the startup of Device1, a connection is established to Device2 via port 5555.
- * Device2 connects to Device3 by using port 5555.
- * Device4 connects to Device1 by using port 5555.

You perform the following actions:

- * Initiate a live response session on Device1 and run the processes command.
- * From Devices in the Microsoft Defender portal, isolate Device1 and Device2.

For each of the following statements, select Yes if True. Otherwise select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 blocks connections from Device4.	☐	☐
Existing connections from Device2 to Device3 are maintained.	☐	☐
The command run in the live response session identifies all the startup processes.	☐	☐

Answer:

Statements	Yes	No
Device1 blocks connections from Device4.	☒	☐
Existing connections from Device2 to Device3 are maintained.	☐	☒
The command run in the live response session identifies all the startup processes.	☒	☐

Explanation:

Answer Area

Statements

Device1 blocks connections from Device4.

Yes

☒

No

☐

Existing connections from Device2 to Device3 are maintained.

☐
☒

The command run in the live response session identifies all the startup processes.

☒
☐

NEW QUESTION: 168

You need to create a query to investigate DNS-related activity. 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

Microsoft

ASim_Dns (where TimeGenerated > ago(7d) | responsecodename='NXDOMAIN')
 ASim_Dns (starttime=ago(7d),
 _Im_Dns (where TimeGenerated > ago(7d) |
 imDns (where TimeGenerated < ago(7d) |

Answer:

Answer Area

Microsoft

ASim_Dns (where TimeGenerated > ago(7d) | responsecodename='NXDOMAIN')
 ASim_Dns (starttime=ago(7d),
 _Im_Dns (where TimeGenerated > ago(7d) |
 imDns (where TimeGenerated < ago(7d) |

Explanation:

Answer Area

ASim_Dns (where TimeGenerated > ago(7d) | responsecodename='NXDOMAIN')
 | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Microsoft

In Microsoft Sentinel, the Advanced Security Information Model (ASIM) provides a standardized schema and parser layer for common telemetry types (DNS, Authentication, NetworkSession, etc.). To investigate DNS-related activity, you should use the ASIM-normalized table ASim_Dns, which unifies data from multiple DNS sources (Microsoft Defender for Endpoint, Azure Firewall, DNS servers, etc.) under a consistent schema.

The ASim_Dns parser standardizes key fields such as:

- * TimeGenerated # timestamp of the DNS event
- * ResponseCodeName # name of the DNS response code (e.g., NXDOMAIN, NOERROR, etc.)
- * QueryName # domain name queried
- * SrcIpAddr and DstIpAddr # IP addresses involved

To investigate recent DNS failures (e.g., non-existent domains), the query filters for events where:

- * TimeGenerated > ago(7d) - limits to the last 7 days of DNS logs.
- * ResponseCodeName == " NXDOMAIN " - identifies DNS lookups that returned "Non-Existent Domain," a common indicator of suspicious or misconfigured activity.

Therefore, the correct and compliant ASIM-based query syntax is:

```
ASim_Dns
| where TimeGenerated > ago(7d)
| where ResponseCodeName == " NXDOMAIN "
```

This approach ensures your investigation leverages ASIM normalization and aligns with Microsoft Sentinel best practices for DNS event analysis.

NEW QUESTION: 169

You have a custom Microsoft Defender XDR detection rule that includes the following KQL query.

```
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
```

For each of the following statements, select Yes if True. Otherwise select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

- 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.

Yes	No
☐	☐
☐	☐
☐	☐

Answer:

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.	☐	☒

NEW QUESTION: 170

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: (SHOW ANSWER)

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

NEW QUESTION: 171

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can assess the repositories in Account1.

What should you do first in the Microsoft Defender for Cloud portal?

- A. Add an environment.

- B.** Enable security policies.
- C.** Enable integrations.
- D.** Enable a plan.

Answer: ([SHOW ANSWER](#))

To allow Microsoft Defender for Cloud to assess GitHub repositories, you must first add GitHub as an environment in the Defender for Cloud portal.

Defender for Cloud supports connecting to external DevOps environments - including GitHub and Azure DevOps - to assess code repositories for security issues such as exposed secrets, vulnerable dependencies, or misconfigurations.

The connection process begins by selecting "Add environment" and then choosing GitHub . After authorization via OAuth to your GitHub account, Defender for Cloud scans the repositories to provide security posture assessments and recommendations.

Other options are not correct because:

- * Enable security policies: Used for configuring compliance and standards within subscriptions, not external code repositories.
 - * Enable integrations: General connector setup, but GitHub integration specifically starts through Add environment .
 - * Enable a plan: Plans (e.g., Defender for Servers, Defender for App Service) control billing and coverage scope, not onboarding.
- # Correct Answer: A. Add an environment

NEW QUESTION: 172

You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.

From Microsoft Sentinel, you investigate a Microsoft 365 incident.

You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.

What should you use?

- A.** the entity side panel of the Timeline card in Microsoft Sentinel
- B.** the investigation graph on the Incidents page of Microsoft Sentinel
- C.** the Timeline tab on the Incidents page of Microsoft Sentinel
- D.** the Alerts page in the Microsoft 365 Defender portal

Answer: ([SHOW ANSWER](#))

Microsoft Sentinel incidents that originate from the Microsoft 365 Defender data connector are synchronized automatically with the Microsoft 365 Defender portal . To add or link an additional alert (for example, from Defender for Cloud Apps) to an existing incident, you must do it from the Microsoft 365 Defender portal's Alerts page , not directly in Sentinel.

Once updated in Microsoft 365 Defender, the changes sync back to Sentinel, maintaining incident parity between both platforms.

Correct Answer: D. the Alerts page in the Microsoft 365 Defender portal

NEW QUESTION: 173

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: ([SHOW ANSWER](#))

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

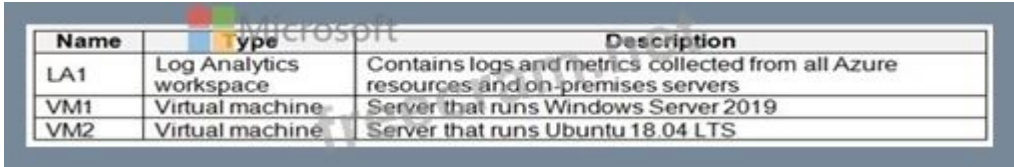
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

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.

NEW QUESTION: 174

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

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

```

Answer:

```

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

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

```

Explanation:

```

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

```

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.

NEW QUESTION: 175

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

You initiated a live response session on Device1.

You need to run a command that will download a 250-MB file named File1.exe from the live response library to Device1. The solution must ensure that File1.exe is downloaded as a background process.

How should you complete the live response command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

< putfile and &

To push (download) a file from the Live Response library onto an endpoint you use the PutFile (often shown as putfile) Live Response command. Microsoft's Live Response command set documents that PutFile "puts a file from the library to the device" and the file is saved to a working folder on the endpoint (and removed on restart by default). This is the operation that transfers a tenant-level library file (for example, an executable you uploaded) onto the target machine for execution or inspection. blog.sec-labs.com+1 When you need the transfer to run as a background job so the live-response session is not blocked waiting for command completion, the Live Response shell supports running commands asynchronously by appending the ampersand operator. Microsoft's Live Response guidance and examples show that background execution is used to avoid blocking the interactive session while large files or long-running operations complete; using & runs the command in the background. Combining these two yields the correct command to download a 250- MB executable from the library to Device1 as a background process: use putfile for the library#device transfer and append & to run it in the background.

Therefore: choose putfile and & .

NEW QUESTION: 176

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.

A screenshot of the Azure Defender configuration interface. It shows two dropdown menus. The first, 'Log Analytics workspace to use:', has options: 'A new Log Analytics workspace in the East US Azure region' (selected), 'Default workspace created by Azure Security Center', and 'LA1'. The second, 'Windows security events to collect:', has options: 'All Events' (selected), 'Common', and 'Minimal'.

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 Group1 that syncs with adatum.com.

All the users at Adatum are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium 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.

NEW QUESTION: 177

You have a Microsoft 365 E5 subscription that is linked to a Microsoft Entra tenant named contoso.com.

You need to query Microsoft Graph activity logs to identify changes to the roles in contoso.com.

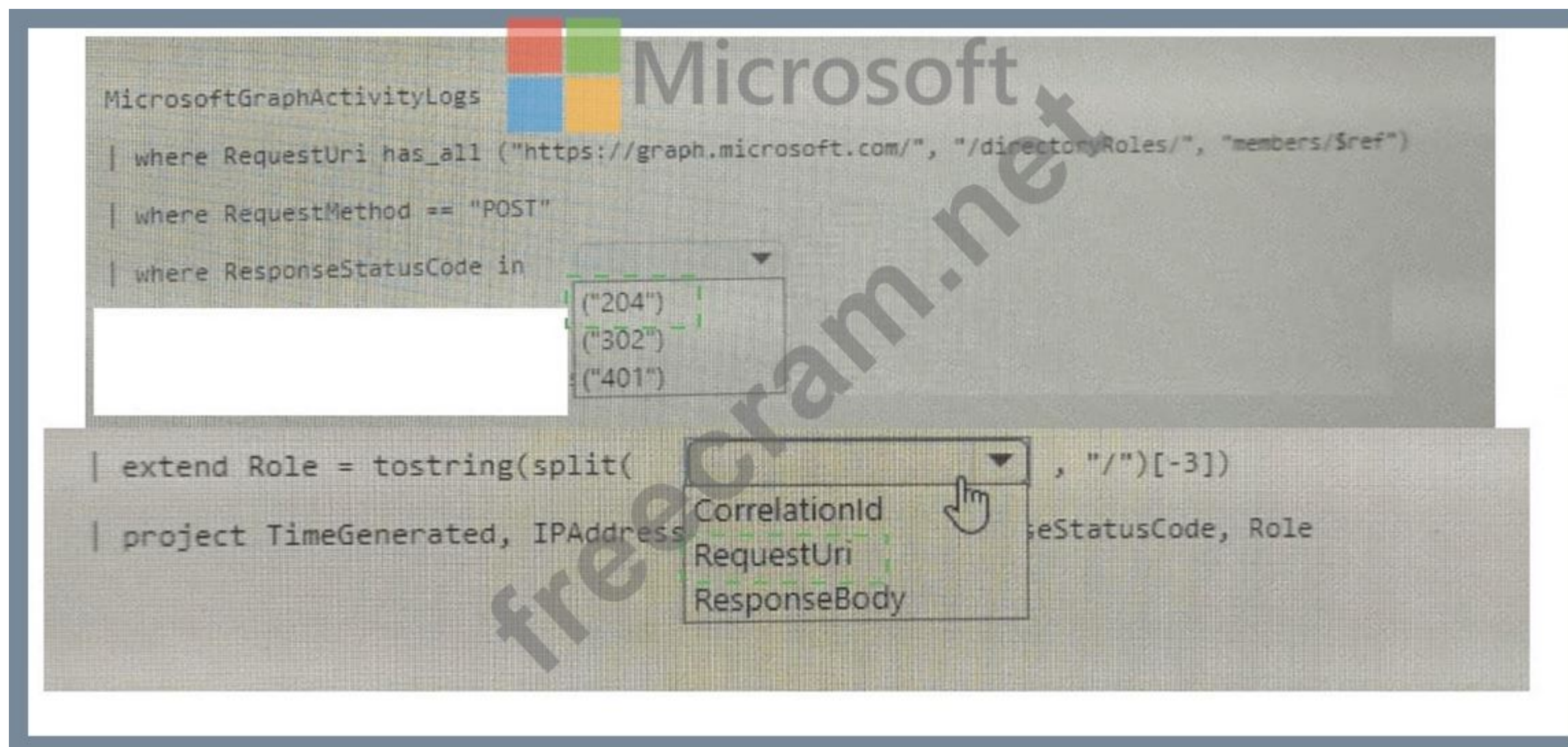
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
MicrosoftGraphActivityLogs
| where RequestUri has_all ("https://graph.microsoft.com/", "/directoryRoles/", "members/$ref")
| where RequestMethod == "POST"
| where ResponseStatusCode in (
    ("204")
    ("302")
    ("401")
)
| extend Role = tostring(split(RequestUri, "/")[-3])
| project TimeGenerated, IPAddress, ResponseStatusCode, Role
```

Microsoft

Answer:



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.

NEW QUESTION: 178

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

- A. executive
- B. sales
- C. marketing

Answer: ([SHOW ANSWER](#))

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.

NEW QUESTION: 179

You have two Microsoft Entra tenants named Tenant1 and Tenant2. Each tenant is linked to an Azure subscription. Tenant1 contains a group named Group1. Tenant2 contains a group named Group2.

You need to implement Microsoft Sentinel for each tenant. The solution must meet the following requirements:

- * Ensure that Group1 can manage security incidents for Tenant1 and Tenant2 in a single workspace.
- * Ensure that Group2 can manage security incidents only for Tenant2.
- * Minimize the use of guest accounts.
- * Minimize administrative effort.
- * Minimize costs.

What should you include in the solution?

- A. one workspace and Privileged Identity Management (PIM)
- B. two workspaces and granular delegated admin privileges (GDAP)
- C. one workspace and multiple role-based access control (RBAC) role assignments
- D. two workspaces and Azure Lighthouse

Answer: ([SHOW ANSWER](#))

Valid SC-200 Dumps shared by EduDump.com for Helping Passing SC-200 Exam! EduDump.com now offer the **newest SC-200 exam dumps**, the EduDump.com SC-200 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-200 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-200/premium/> (**415 Q&As** Dumps, **35%OFF** Special Discount Code: **freecram**)