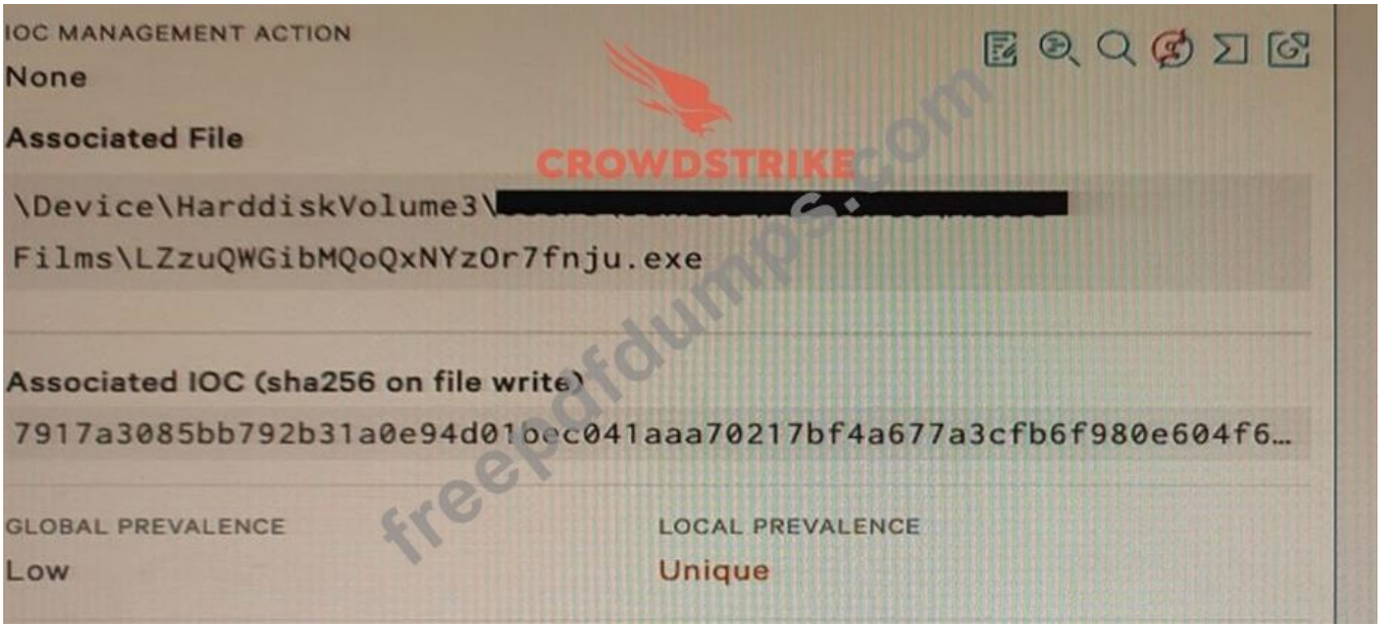
CrowdStrike.CCFH-202.v2023-08-16.q28

Exam Code:	CCFH-202
Exam Name:	CrowdStrike Certified Falcon Hunter
Certification Provider:	CrowdStrike
Free Question Number:	28
Version:	v2023-08-16
# of views:	471
# of Questions views:	280
https://www.freepdfdumps.com/CrowdStrike.CCFH-202.v2023-08-16.q28.html	

NEW QUESTION: 1
Refer to Exhibit.



Falcon detected the above file attempting to execute. At initial glance; what indicators can we use to provide an initial analysis of the file?
A. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled
B. File name, path, Local and Global prevalence within the environment
C. File path, hard disk volume number, and IOC Management action
D. Local prevalence, IOC Management action, and Event Search
Answer: B (LEAVE A REPLY)
The file name, path, Local and Global prevalence are indicators that can provide an initial analysis of the file without relying on external sources or tools. The file name can indicate the purpose or origin of the file, such as if it is a legitimate application or a malicious payload. The file path can indicate where the file was located or executed from, such as if it was in a temporary or system directory. The Local and Global prevalence can indicate how common or rare the file is

within the environment or across all Falcon customers, which can help assess the risk or impact of the file.

NEW QUESTION: 2
What is the main purpose of the Mac Sensor report?
A. To identify endpoints that are in Reduced Functionality Mode
B. To provide a summary view of selected activities on Mac hosts
C. To provide vulnerability assessment for Mac Operating Systems
D. To provide a dashboard for Mac related detections
Answer: B (LEAVE A REPLY)
The Mac Sensor report is a pre-defined report that provides a summary view of selected activities on Mac hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Mac hosts within a specified time range. The Mac Sensor report does not identify endpoints that are in Reduced Functionality Mode, provide vulnerability assessment for Mac Operating Systems, or provide a dashboard for Mac related detections.

NEW QUESTION: 3
Adversaries commonly execute discovery commands such as netexe, ipconfig.exe, and whoami exe. Rather than query for each of these commands individually, you would like to use a single query with all of them. What Splunk operator is needed to complete the following query?

```
aid=my-aid event_simpleName=ProcessRollup2 (FileName=net.exe ________ FileName=ipconfig.exe ________
FileName=whoami.exe) | table ComputerName UserName FileName CommandLine
```

A. OR
B. IN
C. NOT
D. AND
Answer: A (LEAVE A REPLY)
The OR operator is needed to complete the following query, as it allows to search for events that match any of the specified values. The query would look like this: event_simpleName=ProcessRollup2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe The OR operator is used to combine multiple search terms or expressions and return events that match at least one of them. The IN, NOT, and AND operators are not suitable for this query, as they have different functions and meanings.

NEW QUESTION: 4
What topics are presented in the Hunting and Investigation Guide?
A. Detailed tutorial on writing advanced queries such as sub-searches and joins
B. Detailed summary of event names, descriptions, and some key data fields for hunting and investigation
C. Sample hunting queries, select walkthroughs and best practices for hunting with Falcon

D. Recommended platform configurations and prevention settings to ensure detections are generated for hunting leads

Answer: (SHOW ANSWER)

This is the correct answer for the same reason as above. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It does not provide a detailed tutorial on writing advanced queries, a detailed summary of event names and descriptions, or recommended platform configurations and prevention settings.

NEW QUESTION: 5

What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

A. PID

B. Process ID or Parent Process ID

C. CID

D. Process Timeline Link

Answer: (SHOW ANSWER)

The Process Timeline Link is what you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search. The Process Timeline Link is an icon that looks like three horizontal bars with dots on them. It appears next to each process name or ID on various pages in Falcon, such as Hash Search results, Detection details, Event Search results, etc. Clicking on it will open a new tab with the Process Timeline for that process. The PID, the Process ID or Parent Process ID, and the CID are not what you click to jump to a Process Timeline.

NEW QUESTION: 6

What Search page would help a threat hunter differentiate testing, DevOPs, or general user activity from adversary behavior?

A. Hash Search

B. IP Search

C. Domain Search

D. User Search

Answer: D (LEAVE A REPLY)

User Search is a search page that allows a threat hunter to search for user activity across endpoints and correlate it with other events. This can help differentiate testing, DevOPs, or general user activity from adversary behavior by identifying anomalous or suspicious user actions, such as logging into multiple systems, running unusual commands, or accessing sensitive files.

NEW QUESTION: 7

Which of the following is an example of a Falcon threat hunting lead?

A. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories

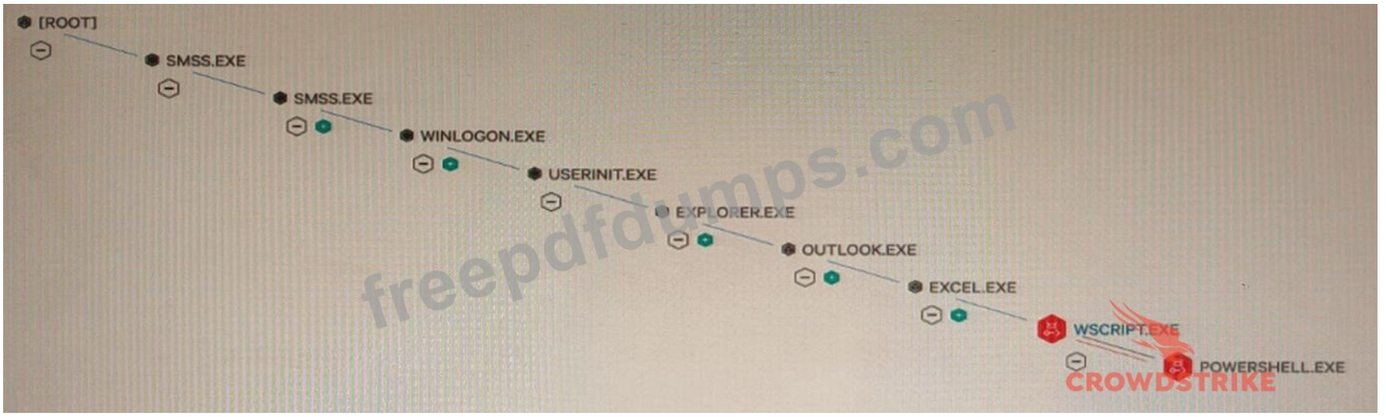
B. Security appliance logs showing potentially bad traffic to an unknown external IP address
C. A help desk ticket for a user clicking on a link in an email causing their machine to become unresponsive and have high CPU usage
D. An external report describing a unique 5 character file extension for ransomware encrypted files
Answer: A (LEAVE A REPLY)
A Falcon threat hunting lead is a piece of information that can be used to initiate or guide a threat hunting activity within the Falcon platform. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories is an example of a Falcon threat hunting lead, as it can indicate potential malicious activity that can be further investigated using Falcon data and features. Security appliance logs, help desk tickets, and external reports are not examples of Falcon threat hunting leads, as they are not directly related to the Falcon platform or data.

NEW QUESTION: 8
When exporting the results of the following event search, what data is saved in the exported file (assuming Verbose Mode)? event_simpleName=*Written | stats count by ComputerName
A. The text of the query
B. The results of the Statistics tab
C. No data Results can only be exported when the "table" command is used
D. All events in the Events tab
Answer: B (LEAVE A REPLY)
When exporting the results of an event search, the data that is saved in the exported file depends on the mode and the tab that is selected. In this case, the mode is Verbose and the tab is Statistics, as indicated by the stats command. Therefore, the data that is saved in the exported file is the results of the Statistics tab, which shows the count of events by ComputerName. The text of the query, all events in the Events tab, and no data are not correct answers.

NEW QUESTION: 9
When performing a raw event search via the Events search page, what are Event Actions?
A. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
B. Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only
C. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search
D. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc
Answer: C (LEAVE A REPLY)

When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon sensor, or the event name defined in the Events Data Dictionary.

NEW QUESTION: 10
Refer to Exhibit.



What type of attack would this process tree indicate?
A. Brute Forcing Attack
B. Man-in-the-middle Attack
C. Phishing Attack
D. Web Application Attack
Answer: (SHOW ANSWER)
This process tree indicates a phishing attack, as it shows a user opening an email attachment (outlook.exe) that launches a malicious macro (cmd.exe) that downloads and executes a payload (powershell.exe) that connects to a remote server (svchost.exe). A phishing attack is a type of social engineering attack that uses deceptive emails or messages to trick users into opening malicious attachments or links that can compromise their systems or credentials.

NEW QUESTION: 11
In the Powershell Hunt report, what does the "score" signify?
A. Number of hosts that ran the PowerShell script
B. How recently the PowerShell script executed
C. Maliciousness score determined by NGAV
D. A cumulative score of the various potential command line switches
Answer: D (LEAVE A REPLY)
In the Powershell Hunt report, the score signifies a cumulative score of the various potential command line switches that were used in the PowerShell script execution. The score is based on a weighted system that assigns different values to different switches based on their potential maliciousness or usefulness for threat hunting. For example, -EncodedCommand has a higher

value than -NoProfile. The score does not signify the number of hosts that ran the PowerShell script, how recently the PowerShell script executed, or the maliciousness score determined by NGAV.

NEW QUESTION: 12
Which document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes?
A. Real Time Response and Network Containment
B. Hunting and Investigation
C. Events Data Dictionary
D. Incident and Detection Monitoring
Answer: (SHOW ANSWER)
The Hunting and Investigation document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes. As explained above, the Hunting and Investigation document is a guide that provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. The other documents do not provide the same information.

NEW QUESTION: 13
You need details about key data fields and sensor events which you may expect to find from Hosts running the Falcon sensor. Which documentation should you access?
A. Events Data Dictionary
B. Streaming API Event Dictionary
C. Hunting and Investigation
D. Event stream APIs
Answer: A (LEAVE A REPLY)
The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because it provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console. The Events Data Dictionary describes each event type, field name, data type, description, and example value that can be used to query and analyze event data. The Streaming API Event Dictionary, Hunting and Investigation, and Event stream APIs are not documentation that provide details about key data fields and sensor events.

NEW QUESTION: 14
Which SPL (Splunk) field name can be used to automatically convert Unix times (Epoch) to UTC readable time within the Flacon Event Search?
A. utc_time
B. conv_time
C. _time

D. time

Answer: C (LEAVE A REPLY)

_time is the SPL (Splunk) field name that can be used to automatically convert Unix times (Epoch) to UTC readable time within the Falcon Event Search. It is a default field that shows the timestamp of each event in a human-readable format. utc_time, conv_time, and time are not valid SPL field names for converting Unix times to UTC readable time.

NEW QUESTION: 15

In the MITRE ATT&CK Framework (version 11 - the newest version released in April 2022), which of the following pair of tactics is not in the Enterprise: Windows matrix?

A. Persistence and Execution

B. Impact and Collection

C. Privilege Escalation and Initial Access

D. Reconnaissance and Resource Development

Answer: D (LEAVE A REPLY)

Reconnaissance and Resource Development are two tactics that are not in the Enterprise: Windows matrix of the MITRE ATT&CK Framework (version 11). These two tactics are part of the PRE-ATT&CK matrix, which covers the actions that adversaries take before compromising a target. The Enterprise: Windows matrix covers the actions that adversaries take after gaining initial access to a Windows system. Persistence, Execution, Impact, Collection, Privilege Escalation, and Initial Access are all tactics that are in the Enterprise: Windows matrix.

NEW QUESTION: 16

What Investigate tool would you use to allow an analyst to view all events for a specific host?

A. Bulk Timeline

B. Host Search

C. Host Timeline

D. Process Timeline

Answer: (SHOW ANSWER)

The Host Timeline is the Investigate tool that you would use to allow an analyst to view all events for a specific host. The Host Timeline shows a graphical representation of all events that occurred on a host within a specified time range. It allows an analyst to zoom in and out, filter by event type or name, and drill down into event details. The Bulk Timeline, the Host Search, and the Process Timeline are not Investigate tools that you would use to view all events for a specific host.

NEW QUESTION: 17
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?
A. Hunting and Investigation
B. Customizable Dashboards
C. MITRE-Based Falcon Detections Framework
D. Events Data Dictionary
Answer: (SHOW ANSWER)
The Hunting and Investigation guide is the Falcon documentation guide that you should reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It covers various topics such as process execution, network connections, registry activity, scheduled tasks, and more.

NEW QUESTION: 18
Where would an analyst find information about shells spawned by root, Kernel Module loads, and wget/curl usage?
A. Sensor Health report
B. Linux Sensor report
C. Sensor Policy Daily report
D. Mac Sensor report
Answer: (SHOW ANSWER)
The Linux Sensor report is where an analyst would find information about shells spawned by root, Kernel Module loads, and wget/curl usage. The Linux Sensor report is a pre-defined report that provides a summary view of selected activities on Linux hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Linux hosts within a specified time range. The Sensor Health report, the Sensor Policy Daily report, and the Mac Sensor report do not provide the same information.

NEW QUESTION: 19
Which of the following best describes the purpose of the Mac Sensor report?
A. The Mac Sensor report displays a listing of all Mac hosts without a Falcon sensor installed
B. The Mac Sensor report provides a detection focused view of known malicious activities occurring on Mac hosts, including machine-learning and indicator-based detections
C. The Mac Sensor report displays a listing of all Mac hosts with a Falcon sensor installed
D. The Mac Sensor report provides a comprehensive view of activities occurring on Mac hosts, including items of interest that may be hunting or investigation leads
Answer: D (LEAVE A REPLY)

This is the correct answer for the same reason as above. The Mac Sensor report provides a comprehensive view of activities occurring on Mac hosts, including items of interest that may be hunting or investigation leads. It does not display a listing of all Mac hosts with or without a Falcon sensor installed, nor does it provide a detection focused view of known malicious activities occurring on Mac hosts.

NEW QUESTION: 20
What is the difference between a Host Search and a Host Timeline?
A. Host Search is used for detection investigation and Host Timeline is used for proactive hunting
B. A Host Search organizes the data in useful event categories like process executions and network connections, a Host Timeline provides an uncategorized view of recorded events in chronological order
C. You access a Host Search from a detection to show you every recorded process event related to the detection and you can only populate the Host Timeline fields manually
D. There is no difference. You just get to them different ways
Answer: B (LEAVE A REPLY)
This is the difference between a Host Search and a Host Timeline. A Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. A Host Timeline is an Investigate tool that allows you to view all events in chronological order, without any categorization. Both tools can be used for detection investigation and proactive hunting, depending on the use case and preference. You can access a Host Search from a detection or manually enter the host details. You can also populate the Host Timeline fields manually or from other pages in Falcon.

NEW QUESTION: 21
Which field in a DNS Request event points to the responsible process?
A. ContextProcessId_readable
B. TargetProcessId_decimal
C. ContextProcessId_decimal
D. ParentProcessId_decimal
Answer: (SHOW ANSWER)
The ContextProcessId_readable field in a DNS Request event points to the responsible process. The ContextProcessId_readable field is the readable representation of the process identifier for the process that initiated the DNS request. It can be used to identify which process was communicating with a specific domain or IP address. The TargetProcessId_decimal, ContextProcessId_decimal, and ParentProcessId_decimal fields do not point to the responsible process.

NEW QUESTION: 22
To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, expand and refer to the _____dashboard panel.

A. Command Line and Admin Tools
B. Processes and Services
C. Registry, Tasks, and Firewall
D. Suspicious File Activity
Answer: (SHOW ANSWER)
To view Files Written to Removable Media within a specified timeframe on a host within the Host Search page, you need to expand and refer to the Suspicious File Activity dashboard panel. The Suspicious File Activity dashboard panel shows information such as files written to removable media, files written to system directories by non-system processes, files written to startup folders, etc. The other dashboard panels do not show files written to removable media.

NEW QUESTION: 23
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct^
A. strftime
B. relative time
C. typeof
D. now
Answer: (SHOW ANSWER)
The strftime eval function is used to convert Unix times (Epoch) into UTC readable time. It takes two arguments: a Unix time field and a format string that specifies how to display the time. The now, typeof, and relative_time eval functions are not used to convert Unix times into UTC readable time.

NEW QUESTION: 24
Which of the following queries will return the parent processes responsible for launching badprogram exe?
A. [search (ParentProcess) where name=badprogranrexe] | table ParentProcessName _time
B. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename ParentProcessId_decimal AS TargetProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
C. [search (ProcessList) where Name=badprogram.exe] | search ParentProcessName | table ParentProcessName _time
D. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename TargetProcessId_decimal AS ParentProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
Answer: D (LEAVE A REPLY)
This query will return the parent processes responsible for launching badprogram.exe by using a subsearch to find the processrollup2 events where FileName is badprogram.exe, then renaming the TargetProcessId_decimal field to ParentProcessId_decimal and using it as a filter for the main

search, then using stats to count the occurrences of each FileName by _time. The other queries will either not return the parent processes or use incorrect field names or syntax.

NEW QUESTION: 25
Which of the following is the proper method to quantify search results, enabling a hunter to quickly sort and identify outliers?
A. Using the "| stats count by" command at the end of a search string in Event Search
B. Using the "|stats count" command at the end of a search string in Event Search
C. Using the "|eval" command at the end of a search string in Event Search
D. Exporting Event Search results to a spreadsheet and aggregating the results
Answer: (SHOW ANSWER)
This is the proper method to quantify search results, enabling a hunter to quickly sort and identify outliers. The stats command is used to calculate summary statistics on the results of a search or subsearch, such as count, sum, average, etc. The count by option is used to count the number of events for each distinct value of a field or fields and display them in a table. This can help find rare or common values that could indicate anomalies or deviations from normal behavior.

NEW QUESTION: 26
Which of the following is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain?
A. Installing a backdoor on the victim endpoint
B. Discovering internet-facing servers
C. Emailing the intended victim with a malware attachment
D. Loading a malicious payload into a common DLL
Answer: B (LEAVE A REPLY)
Discovering internet-facing servers is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain. The RECONNAISSANCE phase is where the adversary researches and identifies targets, vulnerabilities, and attack vectors. Discovering internet-facing servers is a way for the adversary to find potential entry points or weaknesses in the target network.

NEW QUESTION: 27
What information is provided from the MITRE ATT&CK framework in a detection's Execution Details?
A. Grouping Tag
B. Command Line
C. Technique ID
D. Triggering Indicator
Answer: C (LEAVE A REPLY)
Technique ID is the information that is provided from the MITRE ATT&CK framework in a detection's Execution Details. Technique ID is a unique identifier for each technique in the MITRE

ATT&CK framework, such as T1059 for Command and Scripting Interpreter or T1566 for Phishing. Technique ID helps to map a detection to a specific adversary behavior and tactic. Grouping Tag, Command Line, and Triggering Indicator are not information that is provided from the MITRE ATT&CK framework in a detection's Execution Details.

NEW QUESTION: 28
How do you rename fields while using transforming commands such as table, chart, and stats?
A. By renaming the fields with the "rename" command after the transforming command e.g. "stats count by ComputerName | rename count AS total_count"
B. You cannot rename fields as it would affect sub-queries and statistical analysis
C. By using the "renamed" keyword after the field name eg "stats count renamed totalcount by ComputerName"
D. By specifying the desired name after the field name eg "stats count totalcount by ComputerName"
Answer: A (LEAVE A REPLY)
The rename command is used to rename fields while using transforming commands such as table, chart, and stats. It can be used after the transforming command and specify the old and new field names with the AS keyword. You can rename fields as it would not affect sub-queries and statistical analysis, as long as you use the correct field names in your queries. The renamed keyword and the desired name after the field name are not valid ways to rename fields.