Free Questions for CCFH-202 by braindumpscollection

Shared by Maynard on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following queries will return the parent processes responsible for launching badprogram exe?

Options:

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

Explanation:

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.

Question 2

Question Type: MultipleChoice

SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct^

Options:

A- now

B- typeof

C- strftime

D- relative time

Answer:

C

Explanation:

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.

Question 3

Question Type: MultipleChoice

How do you rename fields while using transforming commands such as table, chart, and stats?

Options:

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

Explanation:

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.

Question 4

Question Type: MultipleChoice

Which of the following Event Search queries would only find the DNS lookups to the domain: www randomdomain com?

Options:

A- event_simpleName=DnsRequest DomainName=www randomdomain com

B- event_simpleName=DnsRequest DomainName=randomdomain com ComputerName=localhost

C- Dns=randomdomain com

D- ComputerName=localhost DnsRequest 'randomdomain com'

Answer:

A

Explanation:

This Event Search query would only find the DNS lookups to the domain www randomdomain com, as it specifies the exact event type and domain name to match. The other queries would either find other events or domains that are not relevant to the question.

Question 5

Question Type: MultipleChoice

Event Search data is recorded with which time zone?

Options:

A- PST

B- GMT

C- EST

D- UTC

Answer:

D

Explanation:

Event Search data is recorded with UTC (Coordinated Universal Time) time zone. UTC is a standard time zone that is used as a reference point for other time zones. PST (Pacific Standard Time), GMT (Greenwich Mean Time), and EST (Eastern Standard Time) are not the time zones that Event Search data is recorded with.

Question 6

Question Type: MultipleChoice

Which of the following would be the correct field name to find the name of an event?

Options:

A- Event_SimpleName

B- Event_Simple_Name

C- EVENT_SIMPLE_NAME

D- event_simpleName

Answer:

A

Explanation:

Event_SimpleName is the correct field name to find the name of an event in Falcon Event Search. It is a field that shows the simplified name of each event type, such as ProcessRollup2, DnsRequest, or FileDelete. Event_Simple_Name, EVENT_SIMPLE_NAME, and event_simpleName are not valid field names for finding the name of an event.

Question 7

Question Type: MultipleChoice

Which SPL (Splunk) field name can be used to automatically convert Unix times (Epoch) to UTC readable time within the Flacon Event Search?

Options:

A- utc_time

B- conv_time

C- _time

D- time

Answer:

C

Explanation:

_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.

Question 8

Question Type: MultipleChoice

Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

Options:

A- Model hunting framework

B- Competitive analysis

C- Analysis of competing hypotheses

D- Key assumptions check

Answer:

C

Explanation:

Analysis of competing hypotheses is a structured analytic technique that contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis. It involves listing all the possible hypotheses, identifying the evidence and assumptions for each hypothesis, evaluating the consistency and reliability of the evidence and assumptions, and rating the likelihood of each hypothesis based on the evidence and assumptions.

Question 9

Question Type: **MultipleChoice**

The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when which PowerShell Command line parameter is present?

Options:

A- -Command

B- -Hidden

C- -e

D- -nop

Answer:

A

Explanation:

The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when the -Command parameter is present. The -Command parameter allows PowerShell to execute a specified script block or string. If the script block or string is encoded using Base64 or other methods, the Falcon Detections page will try to decode it and show the original command. The -Hidden, -e, and -nop parameters are not related to encoding or decoding PowerShell commands.

Question 10

Question Type: MultipleChoice

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

Options:

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

Explanation:

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.

Question 11

Question Type: MultipleChoice

A benefit of using a threat hunting framework is that it:

Options:

A- Automatically generates incident reports

B- Eliminates false positives

C- Provides high fidelity threat actor attribution

D- Provides actionable, repeatable steps to conduct threat hunting

Answer:

D

Explanation:

A threat hunting framework is a methodology that guides threat hunters in planning, executing, and improving their threat hunting activities. A benefit of using a threat hunting framework is that it provides actionable, repeatable steps to conduct threat hunting in a consistent and efficient manner. A threat hunting framework does not automatically generate incident reports, eliminate false positives, or provide high fidelity threat actor attribution, as these are dependent on other factors such as data sources, tools, and analysis skills.

To Get Premium Files for CCFH-202 Visit

https://www.p2pexams.com/products/ccfh-202

For More Free Questions Visit

https://www.p2pexams.com/crowdstrike/pdf/ccfh-202