Vendor: CrowdStrike

Exam Code: CCFH-202

Exam Name: CrowdStrike Certified Falcon Hunter

Version: DEMO

QUESTION 1
Which of the following would be the correct field name to find the name of an event?

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 2
Event Search data is recorded with which time zone?

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 3
Which of the following Event Search queries would only find the DNS lookups to the domain: www.randomdomain.com?

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 4
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
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 5
SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time. Which eval function is correct?

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 6
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 ParentProcessld_decimal AS TargetProcessld_decimal | fields aid TargetProcessld_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 TargetProcessld_decimal AS ParentProcessld_decimal | fields aid TargetProcessld_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 TargetProcessld_decimal field to ParentProcessld_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 7

You want to produce a list of all event occurrences along with selected fields such as the full path, time, username etc. Which command would be the appropriate choice?

A. fields
B. distinct count
C. table
D. values

Answer: C
Explanation:
The table command is used to produce a list of all event occurrences along with selected fields such as the full path, time, username etc. It takes one or more field names as arguments and displays them in a tabular format. The fields command is used to keep or remove fields from search results, not to display them in a list. The distinct_count command is used to count the number of distinct values of a field, not to display them in a list. The values command is used to display a list of unique values of a field within each group, not to display all event occurrences.

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
Explanation:
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.