Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CCFH-202 Dumps
CCFH-202 Braindumps
CCFH-202 Real Questions
CCFH-202 Practice Test
CCFH-202 Actual Questions

PASS

CrowdStrike

CCFH-202

CrowdStrike Certified Falcon Hunter (CCFH) Certification

Question: 212

An analyst has sorted all recent detections in the Falcon platform to identify the oldest in an effort to determine the possible first victim host What is this type of analysis called?

A. Visualization of hosts
B. Statistical analysis
C. Temporal analysis
D. Machine Learning

Answer: C

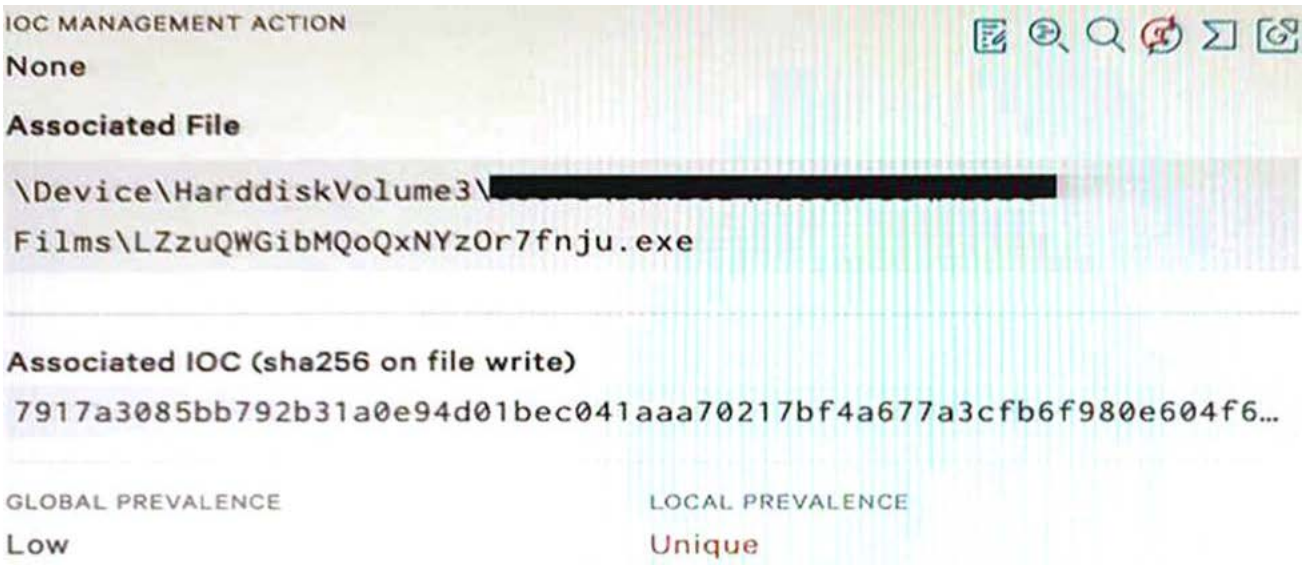
Explanation:

Temporal analysis is a type of analysis that focuses on the timing and sequence of events in order to identify patterns, trends, or anomalies. By sorting all recent detections in the Falcon platform to identify the oldest, an analyst can perform temporal analysis to determine the possible first victim host and trace back the origin of an attack.

Reference: https://www.crowdstrike.com/blog/tech-center/temporal-analysis-in-crowdstrike-falcon/

Question: 213

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

Explanation:

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.

Reference: https://www.crowdstrike.com/blog/tech-center/understanding-file-prevalence-in-crowdstrike-falcon/

Question: 213

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

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.

Reference: https://www.crowdstrike.com/blog/tech-center/threat-hunting-framework/

Question: 214

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

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.

Reference: https://www.crowdstrike.com/blog/tech-center/threat-hunting-leads-in-crowdstrike-falcon/

Question: 215

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

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.

Reference: https://www.crowdstrike.com/blog/tech-center/decoding-powershell-commands-in-crowdstrike-falcon/

Question: 216

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

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.

Reference: https://www.crowdstrike.com/blog/tech-center/analysis-of-competing-hypotheses/

Question: 217

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

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.

Reference: https://www.crowdstrike.com/blog/tech-center/understanding-timestamps-in- crowdstrike-falcon/

Question: 218

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: B

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.

Reference: https://www.crowdstrike.com/blog/tech-center/event-search-in-crowdstrike-falcon/

Question: 219

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.

Reference: https://www.crowdstrike.com/blog/tech-center/understanding-timestamps-in-crowdstrike-falcon/

Question: 220

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

A. event_simpleName=DnsRequestDomainName=www randomdomain com
B. event_simpleName=DnsRequestDomainName=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.

Reference: https://www.crowdstrike.com/blog/tech-center/event-search-in-crowdstrike-falcon/

Question: 221

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.

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/SearchReference/Rename

Question: 222

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.

Reference:https://docs.splunk.com/Documentation/Splunk/8.2.3/SearchReference/CommonEvalFunctions

Question: 223

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: B

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.

Reference: https://www.crowdstrike.com/blog/tech-center/process-rollup-in-crowdstrike-falcon/

Question: 224

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.

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/SearchReference/Table

Question: 225

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.

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.3/Search/Exportsearchresults

Question: 226

The help desk is reporting an increase in calls related to user accounts being locked out over the last few days. You suspect that this could be an attack by an adversary against your organization. Select the best hunting hypothesis from the following:

A. A zero-day vulnerability is being exploited on a Microsoft Exchange server
B. A publicly available web application has been hacked and is causing the lockouts
C. Users are locking their accounts out because they recently changed their passwords
D. A password guessing attack is being executed against remote access mechanisms such as VPN

Answer: D

Explanation:

A hunting hypothesis is a statement that describes a possible malicious activity that can be tested with data and analysis. A good hunting hypothesis should be specific, testable, and relevant to the problem or goal. In this case, the best hunting hypothesis from the following is that a password guessing attack is being executed against remote access mechanisms such as VPN, as it explains the possible cause and method of the user account lockouts in a specific and testable way. A zero-day vulnerability on a Microsoft Exchange server is too vague and does not explain how it relates to the lockouts. A hacked web application is also too vague and does not specify how it causes the lockouts. Users locking their accounts out because they recently changed their passwords is not a malicious activity and does not account for the increase in calls.

Reference: https://www.crowdstrike.com/blog/tech-center/threat-hunting-framework/

Question: 227

To find events that are outliers inside a network,_____is the best hunting method to use.

A. time-based
B. machine learning
C. searching
D. stacking

Answer: D

Explanation:

Stacking (Frequency Analysis) is the best hunting method to use to find events that are outliers inside a network. Stacking involves grouping events by a common attribute and counting their frequency, then sorting them by ascending or descending order to identify rare or common events. This can help find anomalies or deviations from normal behavior that could indicate malicious activity. Time-based searching, machine learning, and searching are not specific hunting methods to find outliers.

Reference: https://www.crowdstrike.com/blog/tech-center/stacking-in-crowdstrike-falcon/

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*