CrowdStrike CCFH-202b Practice Questions

Shared by Pratt on 22-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following best describes the purpose of the Mac Sensor report?

Options:

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

Explanation:

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.

Question 2

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 3

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 4

Question Type: MultipleChoice

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

Options:

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.

Question 5

Question Type: MultipleChoice

While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS " What does this User Name indicate?

Options:

A- The User Name is a System User
B- The User Name is not relevant for the dashboard
C- There is no User Name associated with the event
D- The Falcon sensor could not determine the User Name

Answer:

C

Explanation:

When you see ''hostnameS'' in the User Name column in the Host Search page, it means that there is no User Name associated with the event. This can happen when the event is related to a system process or service that does not have a user context. It does not mean that the User Name is a System User, that the User Name is not relevant for the dashboard, or that the Falcon sensor could not determine the User Name.

Question 6

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.

Question 7

Question Type: MultipleChoice

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?

Options:

A- Events Data Dictionary
B- Streaming API Event Dictionary
C- Hunting and Investigation
D- Event stream APIs

Answer:

A

Explanation:

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.

Question 8

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 9

Question Type: MultipleChoice

Which tool allows a threat hunter to populate and colorize all known adversary techniques in a single view?

Options:

A- MISP
B- OWASP Threat Dragon
C- OpenXDR
D- MITRE ATT&CK Navigator

Answer:

D

Explanation:

MITRE ATT&CK Navigator is a tool that allows a threat hunter to populate and colorize all known adversary techniques in a single view. It is based on the MITRE ATT&CK framework, which is a knowledge base of adversary behaviors and tactics. The tool enables threat hunters to create custom matrices, layers, annotations, and filters to explore and model specific adversary techniques, with links to intelligence and case studies.

Question 10

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 11

Question Type: MultipleChoice

What topics are presented in the Hunting and Investigation Guide?

Options:

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:

C

Explanation:

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.

Question 12

Question Type: MultipleChoice

In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

Options:

A- Prevents command lines containing 'badstring' from being displayed
B- Displays only the command lines containing 'badstring'
C- Highlights 'badstring' in all command lines in the output
D- Highlights only the command lines containing 'badstring'

Answer:

A

Explanation:

In the Powershell Hunt report, the filtering condition of commandLine! ='badstring' prevents command lines containing ''badstring'' from being displayed. The ! operator is used to negate or exclude a condition from the search results. The * operator is used as a wildcard to match any number of characters before or after the specified string. Therefore, commandLine! ='badstring' means to filter out any command line that has ''badstring'' anywhere in it. The other options are not correct, as they do not describe what the filtering condition does.

P2P exams

P2P exams

To Get Premium Files for CCFH-202b Visit

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

For More Free Questions Visit

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

