Free Questions for CCFH-202 by go4braindumps

Shared by Contreras on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the main purpose of the Mac Sensor report?

Options:

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

Explanation:

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.

Question 2

Question Type: MultipleChoice

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?

Options:

A- Real Time Response and Network Containment

B- Hunting and Investigation

C- Events Data Dictionary

D- Incident and Detection Monitoring

Answer:

B

Explanation:

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.

Question 3

Question Type: MultipleChoice

Which of the following does the Hunting and Investigation Guide contain?

Options:

A- A list of all event types and their syntax

B- A list of all event types specifically used for hunting and their syntax

C- Example Event Search queries useful for threat hunting

D- Example Event Search queries useful for Falcon platform configuration

Answer:

C

Explanation:

The Hunting and Investigation guide contains example Event Search queries useful for threat hunting. These queries are based on common threat hunting use cases and scenarios, such as finding suspicious processes, network connections, registry activity, etc. The guide also explains how to customize and modify the queries to suit different needs and environments. The guide does not contain a list of all event types and their syntax, as that information is provided in the Events Data Dictionary. The guide also does not contain example Event Search queries useful for Falcon platform configuration, as that is not the focus of the guide.

Question 4

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 5

Question Type: MultipleChoice

Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

Options:

A- Hunting and Investigation

B- Customizable Dashboards

C- MITRE-Based Falcon Detections Framework

D- Events Data Dictionary

Answer:

A

Explanation:

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.

Question 6

Question Type: MultipleChoice

The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

Options:

A- It provides pre-defined queries you can customize to meet your specific threat hunting needs

B- It provides a list of all the detect names and descriptions found in the Falcon Cloud

C- It provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console

D- It provides a list of compatible splunk commands used to query event data

Answer:

C

Explanation:

This is the correct answer for the same reason as above. The Events Data Dictionary provides a reference of information about the events found in the Investigate > Event Search page of the Falcon Console, which is useful for writing hunting queries. It does not provide pre-defined queries, detect names and descriptions, or compatible splunk commands.

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**

What information is provided from the MITRE ATT&CK framework in a detection's Execution Details?

Options:

A- Grouping Tag

B- Command Line

C- Technique ID

D- Triggering Indicator

Answer:

C

Explanation:

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.