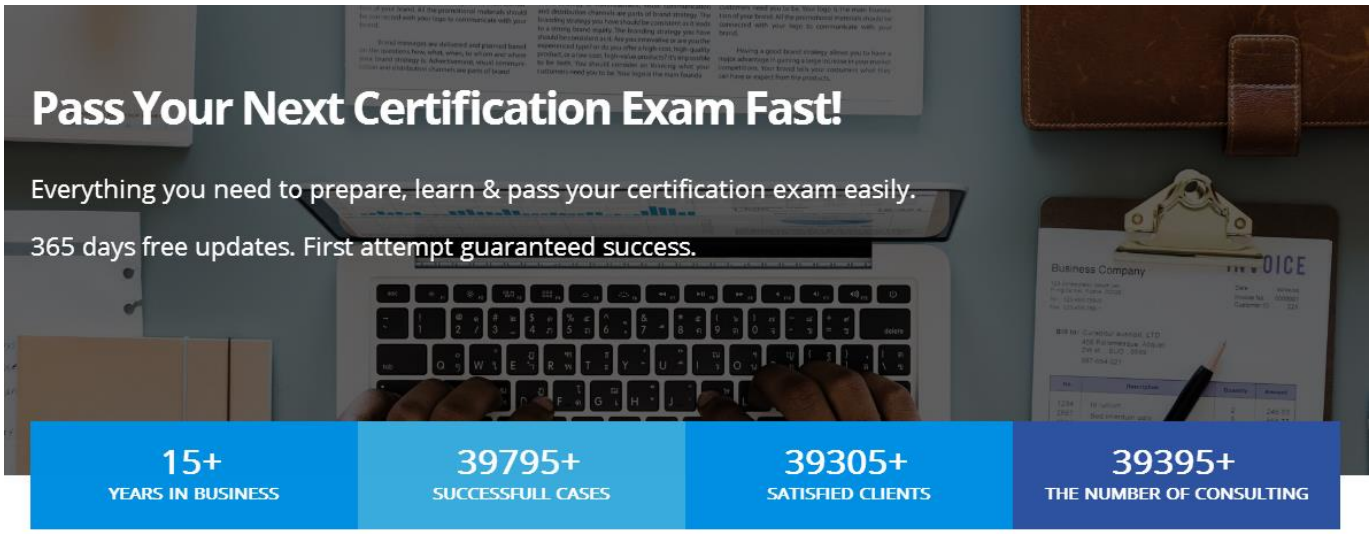
PracticeVCE



TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.practicevce.com

Professional Study Tool and Reliable Exam Practice Material

Exam : **CCFH-202b**

Title : CrowdStrike Certified Falcon Hunter

Vendor : CrowdStrike

Version : DEMO

NO.1 The Events Data Dictionary found in the Falcon documentation is useful for writing hunting queries because:

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.

NO.2 What information is shown in Host Search?

A. Quarantined Files

B. Prevention Policies

C. Intel Reports

D. Processes and Services

Answer: D

Explanation:

Processes and Services is one of the information that is shown in Host Search. Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. Processes and Services is one of the categories that shows information such as process name, command line, parent process name, parent command line, etc. for each process execution event on a host. Quarantined Files, Prevention Policies, and Intel Reports are not shown in Host Search.

NO.3 Which field should you reference in order to find the system time of a *FileWritten event?

A. ContextTimeStamp_decimal

B. FileTimeStamp_decimal

C. ProcessStartTime_decimal

D. timestamp

Answer: A

Explanation:

ContextTimeStamp_decimal is the field that shows the system time of the event that triggered the sensor to send data to the cloud. In this case, it would be the time when the file was written. FileTimeStamp_decimal is the field that shows the last modified time of the file, which may not be the same as the time when the file was written. ProcessStartTime_decimal is the field that shows the start time of the process that performed the file write operation, which may not be the same as the time when the file was written. Timestamp is the field that shows the time when the sensor data was received by the cloud, which may not be the same as the time when the file was written.

NO.4 Which of the following is a suspicious process behavior?

A. PowerShell running an execution policy of RemoteSigned
B. An Internet browser (eg, Internet Explorer) performing multiple DNS requests
C. PowerShell launching a PowerShell script
D. Non-network processes (eg, notepad exe) making an outbound network connection
Answer: D
Explanation:
Non-network processes are processes that are not expected to communicate over the network, such as notepad.exe. If they make an outbound network connection, it could indicate that they are compromised or maliciously used by an adversary. PowerShell running an execution policy of RemoteSigned is a default setting that allows local scripts to run without digital signatures. An Internet browser performing multiple DNS requests is a normal behavior for web browsing. PowerShell launching a PowerShell script is also a common behavior for legitimate tasks.

NO.5 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.

NO.6 Adversaries commonly execute discovery commands such as netexe, ipconfig.exe, and whoami exe. Rather than query for each of these commands individually, you would like to use a single query with all of them. What Splunk operator is needed to complete the following query?

```
aid=my-aid event_simpleName=ProcessRollup2 (FileName=net.exe _______ FileName=ipconfig.exe _______
FileName=whoami.exe) | table ComputerName UserName FileName CommandLine
```

A. OR
B. IN
C. NOT
D. AND
Answer: A
Explanation:
The OR operator is needed to complete the following query, as it allows to search for events that match any of the specified values. The query would look like this:
event_simpleName=ProcessRollup2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe The OR operator is used to combine multiple search terms or expressions and return events that match at least one of them. The IN, NOT, and AND operators are not suitable for this query, as they have different functions and meanings.