CrowdStrike

CCFH-202 Exam

CrowdStrike Certified Falcon Hunter

Thank you for downloading CCFH-202 exam PDF Demo

You can Buy Latest CCFH-202 Full Version Download

https://www.certkillers.net/Exam/CCFH-202

Version: 4.0

Question: 1

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.
Reference: https://www.crowdstrike.com/blog/tech-center/detect-malicious-use-of-non-network-processes/

Question: 2

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

Question: 3

What Search page would help a threat hunter differentiate testing, DevOPs, or general user activity from adversary behavior?

A. Hash Search
B. IP Search
C. Domain Search
D. User Search

Answer: D

Explanation:

User Search is a search page that allows a threat hunter to search for user activity across endpoints and correlate it with other events. This can help differentiate testing, DevOPs, or general user activity from adversary behavior by identifying anomalous or suspicious user actions, such as logging into multiple systems, running unusual commands, or accessing sensitive files.
Reference: https://www.crowdstrike.com/blog/tech-center/user-search-in-crowdstrike-falcon/

Question: 4

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

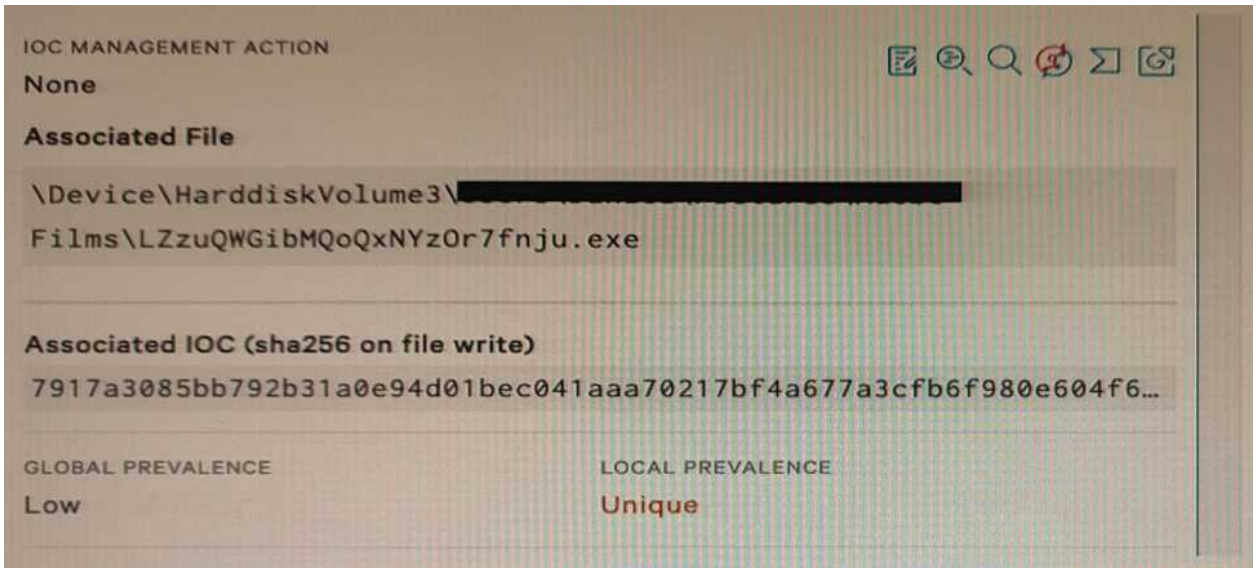
Answer: C

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: 5

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/

Thank You for trying CCFH-202 PDF Demo

To Buy New CCFH-202 Full Version Download visit link below

https://www.certkillers.net/Exam/CCFH-202

Start Your CCFH-202 Preparation

Use Coupon “CKNET” for Further discount on the purchase of Full Version Download. Test your CCFH-202 preparation with exam questions.