DUMPSHQ

Free Questions for CCFH-202 by dumpshq

Shared by Morse on 09-08-2024

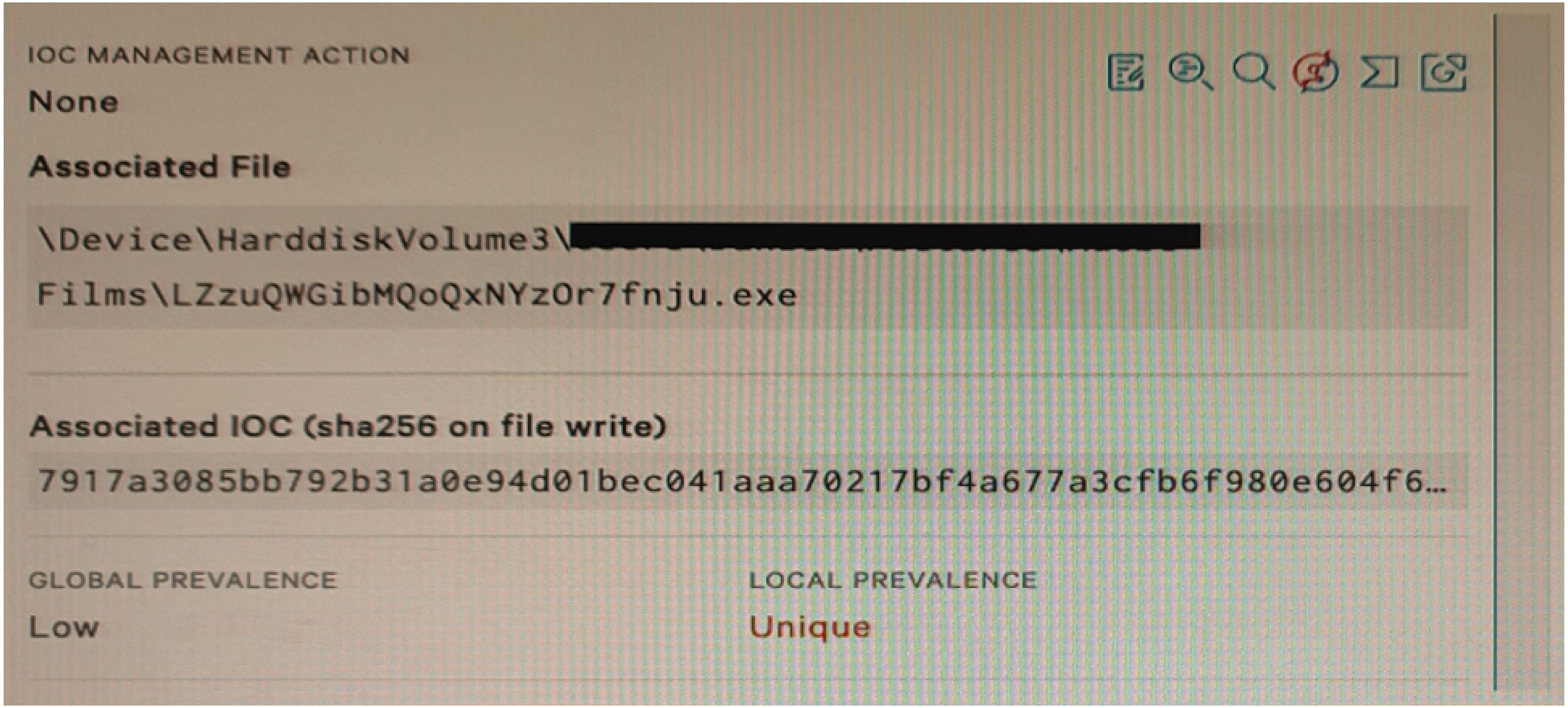
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to Exhibit.



IOC MANAGEMENT ACTION

None

Associated File

```
\Device\HarddiskVolume3\[redacted]
Films\LZzuQWGibMQoQxNYzOr7fnju.exe
```

Associated IOC (sha256 on file write)

```
7917a3085bb792b31a0e94d01bec041aaa70217bf4a677a3cfb6f980e604f6...
```

GLOBAL PREVALENCE

Low

LOCAL PREVALENCE

Unique

Falcon detected the above file attempting to execute. At initial glance; what indicators can we use to provide an initial analysis of the file?

Options:

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.

Question 2

Question Type: MultipleChoice

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?

Options:

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.

Question 3

Question Type: MultipleChoice

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

Options:

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.

Question 4

Question Type: MultipleChoice

Which field should you reference in order to find the system time of a *FileWritten event?

Options:

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.

Question 5

Question Type: **MultipleChoice**

Which of the following is a suspicious process behavior?

Options:

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.

Question 6

Question Type: MultipleChoice

Which of the following is TRUE about a Hash Search?

Options:

A- Wildcard searches are not permitted with the Hash Search

B- The Hash Search provides Process Execution History

C- The Hash Search is available on Linux

D- Module Load History is not presented in a Hash Search

Answer:

B

Explanation:

The Hash Search is an Investigate tool that allows you to search for a file hash and view its process execution history across all hosts in your environment. It shows information such as process name, command line, parent process name, parent command line, etc. for each execution of the file hash. Wildcard searches are permitted with the Hash Search, as long as they are at least four characters long. The Hash Search is available on Linux, as well as Windows and Mac OS X. Module Load History is presented in a Hash Search, along with other information such as File Write History and Detection History.

Question 7

Question Type: MultipleChoice

In the MITRE ATT&CK Framework (version 11 - the newest version released in April 2022), which of the following pair of tactics is not in the Enterprise: Windows matrix?

Options:

A- Persistence and Execution

B- Impact and Collection

C- Privilege Escalation and Initial Access

D- Reconnaissance and Resource Development

Answer:

D

Explanation:

Reconnaissance and Resource Development are two tactics that are not in the Enterprise: Windows matrix of the MITRE ATT&CK Framework (version 11). These two tactics are part of the PRE-ATT&CK matrix, which covers the actions that adversaries take before compromising a target. The Enterprise: Windows matrix covers the actions that adversaries take after gaining initial access to a Windows system. Persistence, Execution, Impact, Collection, Privilege Escalation, and Initial Access are all tactics that are in the Enterprise: Windows matrix.

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.

Question 9

Question Type: MultipleChoice

You are reviewing a list of domains recently banned by your organization's acceptable use policy. In particular, you are looking for the number of hosts that have visited each domain. Which tool should you use in Falcon?

Options:

A- Create a custom alert for each domain

B- Allowed Domain Summary Report

C- Bulk Domain Search

D- IP Addresses Search

Answer:

C

Explanation:

Bulk Domain Search is the tool that you should use in Falcon to review a list of domains recently banned by your organization's acceptable use policy and look for the number of hosts that have visited each domain. Bulk Domain Search is an Investigate tool that allows you to search for multiple domains at once and view their network connection events across all hosts in your environment. It shows information such as domain name, number of hosts visited, number of detections generated, etc. for each domain. Create a custom alert for each domain, Allowed Domain Summary Report, and IP Addresses Search are not tools that you should use for this purpose.

Question 10

Question Type: **MultipleChoice**

In the Powershell Hunt report, what does the "score" signify?

Options:

A- Number of hosts that ran the PowerShell script

B- How recently the PowerShell script executed

C- Maliciousness score determined by NGAV

D- A cumulative score of the various potential command line switches

Answer:

D

Explanation:

In the Powershell Hunt report, the score signifies a cumulative score of the various potential command line switches that were used in the PowerShell script execution. The score is based on a weighted system that assigns different values to different switches based on their potential maliciousness or usefulness for threat hunting. For example, -EncodedCommand has a higher value than -NoProfile. The score does not signify the number of hosts that ran the PowerShell script, how recently the PowerShell script executed, or the maliciousness score determined by NGAV.

20%
DISCOUNT