Download CrowdStrike CCFH-202b Exam Dumps Free

Shared by Graves on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which option best Event Search queries would only find the DNS lookups to the domain: www randomdomain com?

Options:

A- event_simpleName=DnsRequest DomainName=www randomdomain com
B- event_simpleName=DnsRequest DomainName=randomdomain com ComputerName=localhost
C- Dns=randomdomain com
D- ComputerName=localhost DnsRequest 'randomdomain com'

Answer:

A

Explanation:

This Event Search query would only find the DNS lookups to the domain www randomdomain com, as it specifies the exact event type and domain name to match. The other queries would either find other events or domains that are not relevant to the question.

Question 2

Question Type: MultipleChoice

SPL (Splunk) eval statements can be used to convert Unix times (Epoch) into UTC readable time Which eval function is correct^

Options:

A- now
B- typeof
C- strftime
D- relative time

Answer:

C

Explanation:

The strftime eval function is used to convert Unix times (Epoch) into UTC readable time. It takes two arguments: a Unix time field and a format string that specifies how to display the time. The now, typeof, and relative_time eval functions are not used to convert Unix times into UTC readable time.

Question 3

Question Type: MultipleChoice

When performing a raw event search via the Events search page, what are Event Actions?

Options:

A- Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
B- Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process from executing or taking no actions and creating a detection only
C- Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search
D- Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc

Answer:

C

Explanation:

When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon

sensor, or the event name defined in the Events Data Dictionary.

Question 4

Question Type: MultipleChoice

To find events that are outliers inside a network,_____is the best hunting method to use.

Options:

A- time-based
B- machine learning
C- searching
D- stacking

Answer:

D

Explanation:

Stacking (Frequency Analysis) is the best hunting method to use to find events that are outliers inside a network. Stacking involves grouping events by a common attribute and counting their frequency, then sorting them by ascending or descending order to identify rare or common events. This can help find anomalies or deviations from normal behavior that could indicate malicious activity. Time-based searching, machine learning, and searching are not specific hunting methods to find outliers.

Question 5

Question Type: MultipleChoice

Which pre-defined reports offer information surrounding activities that typically indicate suspicious activity occurring on a system?

Options:

A- Scheduled searches
B- Hunt reports
C- Sensor reports
D- Timeline reports

Answer:

B

Explanation:

Hunt reports are pre-defined reports that offer information surrounding activities that typically indicate suspicious activity occurring on a system. They are based on common threat hunting use cases and queries, and they provide visualizations and summaries of the results. Hunt reports can help threat hunters quickly identify and investigate potential threats in their environment.

Question 6

Question Type: MultipleChoice

Event Search data is recorded with which time zone?

Options:

A- PST
B- GMT
C- EST
D- UTC

Answer:

D

Explanation:

Event Search data is recorded with UTC (Coordinated Universal Time) time zone. UTC is a standard time zone that is used as a reference point for other time zones. PST (Pacific Standard Time), GMT (Greenwich Mean Time), and EST (Eastern Standard Time) are not the time zones that Event Search data is recorded with.

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

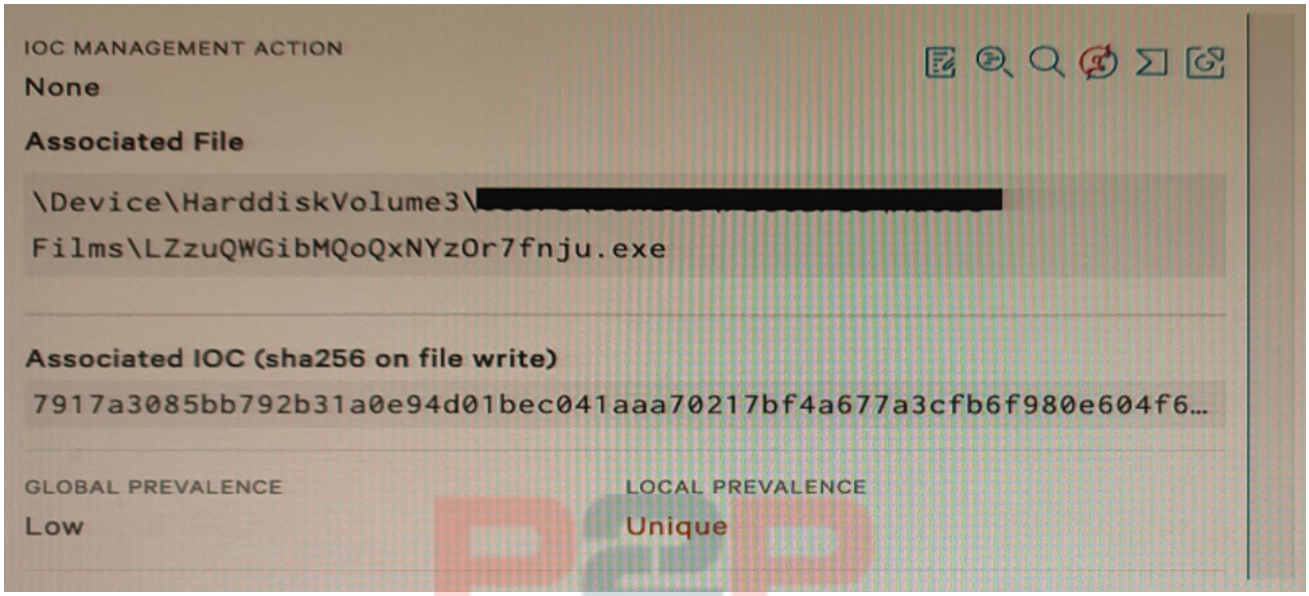
Explanation:

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

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?

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.