CCFH-202b Exam Questions Pdf, CCFH-202b Prepaway Dumps

This is a portable file that contains the most probable CCFH-202b test questions. The CrowdStrike CCFH-202b PDF dumps format is a convenient preparation method as these CrowdStrike CCFH-202b questions document is printable and portable. You can use this format of the CrowdStrike CCFH-202b Exam product for quick study and revision. Laptops, tablets, and smartphones support the CCFH-202b dumps PDF files.

Passing CCFH-202b certification can help you realize your dreams. If you buy our product, we will provide you with the best CCFH-202b study materials and it can help you obtain CCFH-202b certification. Our CCFH-202b exam braindump is of high quality and our service is perfect. With our proved data from our loyal customers that the pass rate of our CCFH-202b Practice Engine is as high as 99% to 100%. Your success is insured with our excellent CCFH-202b training questions.

>> CCFH-202b Exam Questions Pdf <<

CCFH-202b Prepaway Dumps | New Soft CCFH-202b Simulations

Don't waste much more time on preparing for a test. Hurry to purchase ValidDumps CrowdStrike CCFH-202b certification training dumps. With the exam dumps, you will know how to effectively prepare for your exam. This is precious tool that can let you sail through CCFH-202b test with no mistakes. Missing the chance, I am sure you must regret it. Thus, don't hesitate and act quickly.

CrowdStrike Certified Falcon Hunter Sample Questions (Q24-Q29):

NEW QUESTION # 24
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

- A. MITRE-Based Falcon Detections Framework
- B. Hunting and Investigation
- C. Events Data Dictionary
- D. Customizable Dashboards

Answer: B

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.

NEW QUESTION # 25
In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

- A. Weaponization
- B. Command & control
- C. Exploitation
- D. Installation

Answer: A

Explanation:
Weaponization is the stage of the Cyber Kill Chain where the actor does not interact with the victim endpoint(s). Weaponization is where the actor prepares or packages the exploit or payload that will be used to compromise the target. This stage does not involve any communication or interaction with the victim endpoint(s), as it is done by the actor before delivering the weaponized content. Exploitation, Command & Control, and Installation are all stages where the actor interacts with the victim endpoint(s), either by executing code, establishing communication, or installing malware.

NEW QUESTION # 26
Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

- A. Analysis of competing hypotheses
- B. Model hunting framework
- C. Competitive analysis
- D. Key assumptions check

Answer: A

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.

NEW QUESTION # 27
When performing a raw event search via the Events search page, what are Event Actions?

- A. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc
- B. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
- 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 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

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.

NEW QUESTION # 28
You would like to search for ANY process execution that used a file stored in the Recycle Bin on a Windows host. Select the option to complete the following EAM query.

- A.