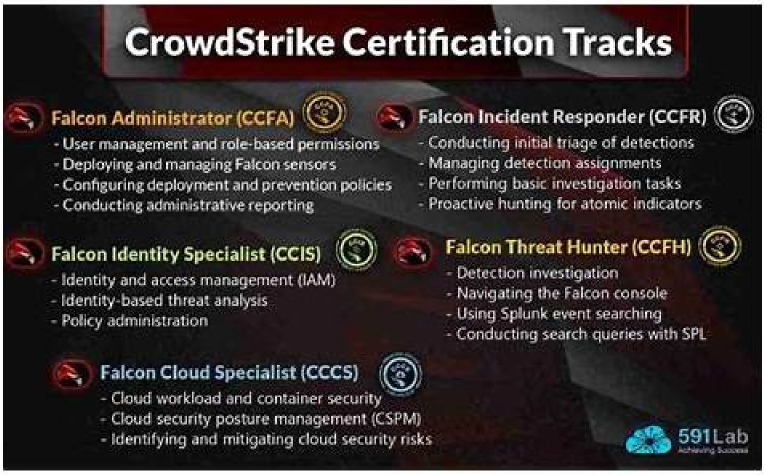
Free PDF High Pass-Rate CrowdStrike - CCFH-202b - Test CrowdStrike Certified Falcon Hunter Lab Questions



CrowdStrike Certification Tracks

Falcon Administrator (CCFA)
- User management and role-based permissions
- Deploying and managing Falcon sensors
- Configuring deployment and prevention policies
- Conducting administrative reporting

Falcon Incident Responder (CCFR)
- Conducting initial triage of detections
- Managing detection assignments
- Performing basic investigation tasks
- Proactive hunting for atomic indicators

Falcon Identity Specialist (CCIS)
- Identity and access management (IAM)
- Identity-based threat analysis
- Policy administration

Falcon Threat Hunter (CCFH)
- Detection investigation
- Navigating the Falcon console
- Using Splunk event searching
- Conducting search queries with SPL

Falcon Cloud Specialist (CCCS)
- Cloud workload and container security
- Cloud security posture management (CSPM)
- Identifying and mitigating cloud security risks

591Lab

before making a choice, you can download a trial version of CCFH-202b preparation materials. After you use it, you will have a more complete understanding of this CCFH-202b exam questions. In this way, you can use our CCFH-202b study materials in a way that suits your needs and professional opinions. We hope you will have a great experience with CCFH-202b Preparation materials. At the same time, we also hope that you can realize your dreams with our help. We will be honored.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 2	• Event Search: This domain focuses on using CrowdStrike Query Language to build queries, format and filter event data, understand process relationships and event types, and create custom dashboards.
Topic 3	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 4	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 5	• Hunting Analytics: This domain focuses on recognizing malicious behaviors, evaluating information reliability, decoding command line activity, identifying infection patterns, distinguishing legitimate from adversary activity, and identifying exploited vulnerabilities.

>> Test CCFH-202b Lab Questions <<

Comprehensive CrowdStrike CCFH-202b Questions in PDF Format

Among all substantial practice materials with similar themes, our CCFH-202b practice materials win a majority of credibility for promising customers who are willing to make progress in this line. With excellent quality at attractive price, our CCFH-202b Exam Questions get high demand of orders in this fierce market. You can just look at the data about the hot hit on the CCFH-202b study braindumps everyday, and you will know that how popular our CCFH-202b learning guide is.

CrowdStrike Certified Falcon Hunter Sample Questions (Q12-Q17):

NEW QUESTION # 12
What information is provided from the MITRE ATT&CK framework in a detection's Execution Details?

- A. Command Line
- B. Triggering Indicator
- C. Grouping Tag
- D. Technique ID

Answer: D

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.

NEW QUESTION # 13
Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

- A. MITRE ATT&CK
- B. NIST 800-171 Cyber Threat Framework
- C. Lockheed Martin Cyber Kill Chain
- D. Director of National Intelligence Cyber Threat Framework

Answer: A

Explanation:
MITRE ATT&CK is a threat framework that allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies. It is a knowledge base of adversary behaviors and tactics that covers various platforms, domains, and scenarios. It provides a common language and structure for threat hunters to understand and analyze threats, as well as to share findings and recommendations.

NEW QUESTION # 14
Which document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes?

- A. Incident and Detection Monitoring
- B. Hunting and Investigation
- C. Real Time Response and Network Containment
- D. Events Data Dictionary

Answer: B

Explanation:
The Hunting and Investigation document provides information on best practices for writing Splunk-based hunting queries, predefined queries which may be customized to hunt for suspicious network connections, and predefined queries which may be customized to hunt for suspicious processes. As explained above, the Hunting and Investigation document is a guide that provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. The other documents do not provide the same information.

NEW QUESTION # 15
The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when which PowerShell Command line parameter is present?

- A. -nop
- B. -e

- C. -Hidden
- D. -Command

Answer: D

Explanation:
The Falcon Detections page will attempt to decode Encoded PowerShell Command line parameters when the -Command parameter is present. The -Command parameter allows PowerShell to execute a specified script block or string. If the script block or string is encoded using Base64 or other methods, the Falcon Detections page will try to decode it and show the original command. The -Hidden, -e, and -nop parameters are not related to encoding or decoding PowerShell commands.

NEW QUESTION # 16
Which field should you reference in order to find the system time of a *FileWritten event?

- A. ProcessStartTime_decimal
- B. FileTimeStamp_decimal
- C. timestamp
- D. ContextTimeStamp_decimal

Answer: D

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.

NEW QUESTION # 17
......

By attempting these CrowdStrike Certified Falcon Hunter (CCFH-202b) mock exams, you can enhance your confidence and overcome weaknesses. The CCFH-202b desktop software of TestSimulate works offline on Windows computers. The web-based CrowdStrike CCFH-202b Practice Exam is compatible with all operating systems and browsers.

CCFH-202b Test Pattern: https://www.testsimulate.com/CCFH-202b-study-materials.html and download exam materials for free through 《 www.examdiscuss.com 》 □Accurate CCFH-202b Test

- CrowdStrike CCFH-202b Pre-Exam Practice Tests | Pdfvce □ Search for □ CCFH-202b □ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □Study CCFH-202b Group
- Why the CrowdStrike CCFH-202b Certification Matters □ Open ➡ www.examdiscuss.com □□□ and search for ➡ CCFH-202b □□□ to download exam materials for free □CCFH-202b Latest Exam Online
- genai-training.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, academy.rebdaa.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes