# Free PDF 2026 CrowdStrike CCFR-201b: Efficient New CrowdStrike Certified Falcon Responder Test Simulator


Your purchase with PrepAwayETE is safe and fast. We use Paypal for payment and committed to keep your personal information secret and never share your information to the third part without your permission. In addition, our CrowdStrike CCFR-201b practice exam torrent can be available for immediate download after your payment. Besides, we guarantee you 100% pass for CCFR-201b Actual Test, in case of failure, you can ask for full refund. The refund procedure is very easy. You just need to show us your CCFR-201b failure certification, then after confirmation, we will deal with your case.

Our CCFR-201b exam torrent is available in PDF, software, and online three modes, which allowing you to switch learning materials on paper, on your phone or on your computer, and to study anywhere and anytime with the according version of CCFR-201b practice test. Before you purchase the system, CCFR-201b Practice Test provides you with a free trial service, so that customers can fully understand our system before buying; after the online payment is successful, you can receive mail from customer service in 5 to 10 minutes, and then immediately begin to learn CCFR-201b training prep.

**>> New CCFR-201b Test Simulator <<**

## CCFR-201b Latest Mock Test & CCFR-201b 100% Exam Coverage

When you are studying for the CCFR-201b exam, maybe you are busy to go to work, for your family and so on. Time is precious for everyone to do the efficient job. If you want to get good CCFR-201b prep guide, it must be spending less time to pass it. We are choosing the key point and the latest information to finish our CCFR-201b Guide Torrent. It only takes you 20 hours to 30 hours to do the practice. After your effective practice, you can master the examination point from the CCFR-201b exam torrent. Then, you will have enough confidence to pass the CCFR-201b exam.

## CrowdStrike CCFR-201b Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Detection Analysis: This domain covers analyzing and triaging detections in Falcon, including interpreting dashboards, endpoint detections, contextual data, process views, prevalence, IOCs, and implementing hash management actions like blocking, allowlisting, and exclusions. |
| Topic 2 | • Event Investigation: This domain covers analyzing Process and Host Timelines, pivoting to Process Timeline or Process Explorer, and analyzing process relationships using Full Detection Details. |
| Topic 3 | • Search Tools: This domain covers utilizing User Search, IP Search, Hash Search, Host Search, and Bulk Domain Search to gather intelligence during investigations. |

| | |
|---|---|
| Topic 4 | • Event Search: This domain focuses on performing advanced event searches from detections, refining searches using event actions, and distinguishing between commonly used event types. |

## CrowdStrike Certified Falcon Responder Sample Questions (Q132-Q137):

**NEW QUESTION # 132**
A responder has identified a suspicious PowerShell script executing on a domain controller. To perform a deep-dive forensic analysis of every action taken by that specific process-including network connections and file modifications-the analyst needs to pivot to a Process Timeline. What is the absolute minimum telemetry data required to generate this auto-filled view?

- A. Agent ID (AID) and Local IP Address
- B. Hostname and MAC Address
- C. Agent ID (AID) and Target Process ID (TargetProcessId_decimal)
- D. User SID and SHA256 Hash

**Answer: C**

**NEW QUESTION # 133**
You are reviewing the raw data in an event search from a detection tree. You find a FileOpenInfo event and want to find out if any other files were opened by the responsible process. Which two field values do you need from this event to perform a Process Timeline search?

- A. ResponsibleProcessId_decimal and aid
- B. TargetProcessId_decimal and aid
- C. ContextProcessId_decimal and aid
- D. ParentProcessId_decimal and aid

**Answer: B**

**NEW QUESTION # 134**
The Activity Dashboard is a core feature for security teams. What is the primary purpose of this dashboard?

- A. To manage the installation and update of Falcon sensors.
- B. To view the raw telemetry of every event happening on the network.
- C. To audit the changes made by other Falcon administrators.
- D. To provide a summary of the current threat state and active detections in the environment.

**Answer: D**

**NEW QUESTION # 135**
Which of the following is NOT a valid event type?

- A. StartofProcess
- B. ProcessRollup2
- C. EndofProcess
- D. DnsRequest

**Answer: C**

**NEW QUESTION # 136**
During an advanced hunting session, a responder is writing a custom query in the Event Search tool to track the lineage of a suspicious process. They notice a field labeled TargetProcessId_decimal. Which of the following sentences accurately describes the technical significance of this value within the CrowdStrike telemetry ecosystem?

- A. It is the standard Process ID (PID) assigned by the Windows Task Manager.
- B. It represents the memory offset where the process's primary thread began.
- C. It is a count of the total number of child processes spawned by that executable.
- D. It is a sensor-assigned, environment-wide unique decimal identifier for that specific process instance.

**Answer: D**

**NEW QUESTION # 137**

.....

CCFR-201b Guide Quiz helped over 98 percent of exam candidates get the certificate. Before you really attend the CrowdStrike CCFR-201b exam and choose your materials, we want to remind you of the importance of holding a certificate like this one. Obtaining a CrowdStrike CCFR-201b certificate likes this one can help you master a lot of agreeable outcomes in the future, like higher salary, the opportunities to promotion and being trusted by the superiors and colleagues.