3-Day Table of Contents for CCFR (CrowdStrike Certified Falcon Responder)

Day 1: Introduction and ATT&CK Framework Application

- **1.0 ATT&CK Framework Application**
  - **1.1** Understanding the MITRE ATT&CK framework and its relevance to Falcon.
  - **1.2** Applying ATT&CK tactics and techniques within Falcon for detection context.
- **2.0 Detection Analysis (Part 1)**
  - **2.1** Recommending courses of action based on Falcon analysis.
  - **2.2** Interpreting information in the Endpoint Security > Activity Dashboard.
  - **2.3** Interpreting information in Endpoint Security > Endpoint Detections.
  - **2.4** Determining an appropriate response based on detection source.
- **Practical Exercises (Hands On)**
  - Overview of MITRE ATT&CK within Falcon.
  - Hands-on exercises with Falcon's detection dashboard and response actions.

Day 2: Detection Analysis (Part 2) and Event Search

- **2.0 Detection Analysis (Part 2)**
  - **2.5** Understanding OSINT tools and their use cases.
  - **2.6** Contextual event data in a detection (IP/DNS/Disk/etc.).
  - **2.7** Triage and analysis of detections using filtering, grouping, and sorting.
  - **2.8** Evaluating internal and external prevalence of threats.
  - **2.9** Full detection view analysis and appropriate response.
  - **2.10** Interpreting data in Process Tree, Process Table, and Process Activity views.
  - **2.11** Host search for identifying managed/unmanaged neighbors.
  - **2.12** Understanding IOCs and available actions in Falcon.
  - **2.13** Using hash management actions effectively.
  - **2.14** Allowlisting and blocklisting effects.
  - **2.15** Effects of machine learning exclusions, sensor visibility, and IOA exclusions.
  - **2.16** Best practices for quarantined files.
- **3.0 Event Search**
  - **3.1** Performing an advanced search and refining it with event actions.
  - **3.2** Determining the best event actions based on context.
  - **3.3** Common event types and their significance.
- **Practical Exercises (Hands On)**
  - Detections triage and advanced event search practices.

Day 3: Event Investigation, Search Tools, and Real-Time Response

- **4.0 Event Investigation**
  - **4.1** Information provided by a Process Timeline.
  - **4.2** Information provided by a Hosts Timeline.
  - **4.3** When to pivot to a Process Timeline or Process Explorer.
  - **4.4** Analyzing process relationships (parent/child/sibling) in Full Detection Details.
- **5.0 Search Tools**
  - **5.1** User search analysis.
  - **5.2** IP search analysis.
  - **5.3** Hash search analysis.
  - **5.4** Host search result interpretation.
  - **5.5** Bulk domain search analysis.
- **6.0 Real-Time Response (RTR)**
  - **6.1** Understanding RTR technical capabilities.
  - **6.2** Identifying RTR administrative requirements.
  - **6.3** Connecting to a host using RTR.
  - **6.4** Investigating threats using RTR commands.
  - **6.5** Using custom scripts in RTR for remediation.
  - **6.6** Setting up workflows with RTR custom scripts.
  - **6.7** Auditing RTR activities using audit logs.
- **Practical Exercises (Lab)**
  - Event investigation and usage of real-time response tools with Falcon.