2-Day Table of Contents for CCFA (CrowdStrike Certified Falcon Administrator) Exam Preparation

---

Day 1: User and Sensor Management, Host Setup, and Group Creation

- **1.0 User Management**
  - **1.1** Determine roles required for access to Falcon console features.
  - **1.2** Create roles and assign users based on permissions.
  - **1.3** Manage API Keys for user and system access.
- **2.0 Sensor Deployment**
  - **2.1** Prerequisites for successful sensor installation on supported OS.
  - **2.2** Analyze default policies and best practices for preparing workloads.
  - **2.3** Uninstall a Falcon sensor.
  - **2.4** Troubleshoot sensor issues and resolution strategies.
- **3.0 Host Management & Setup**
  - **3.1** Using filters in the Host Management page.
  - **3.2** Disabling detections for a host and understanding its impact.
  - **3.3** Reduced Functionality Mode (RFM) impact and causes.
  - **3.4** Finding hosts in RFM and locating inactive sensors.
  - **3.5** Retention time for inactive sensors.
  - **3.6** Relevant reports for host management.
- **4.0 Group Creation**
  - **4.1** Assigning endpoints to appropriate groups and their policy implications.
  - **4.2** Best practices for managing host groups.
- **Practical Exercises (Hands On)**
  - Hands-on with user roles, sensor deployment, and group creation in Falcon.

Day 2: Policy Application, Rule Configuration, Dashboards, and Workflows

- **5.0 Policy Application**
  - **5.1** Prevention policy settings and their effect on security posture.
  - **5.2** Sensor update policy settings to manage update processes.
  - **5.3** Role and policy settings management, reviewing RTR audit logs.
  - **5.4** Understanding containment policies and security workflow requirements.
  - **5.5** Configuring containment policies for IP or subnet exclusions.
  - **5.6** Managing quarantined files and understanding policy options.
- **6.0 Rule Configuration**
  - **6.1** Creating custom IOA rules for non-malicious behavior monitoring.
  - **6.2** Interpreting business requirements to resolve false positives.
  - **6.3** Configuring IOC settings for customized security postures.

    - **6.4** Managing configurations across the CID in General Settings.
- **7.0 Dashboards and Reports**
    - **7.1** Understanding sensor reports and their use cases.
    - **7.2** Audit logs and their significance in monitoring activity.
- **8.0 Workflows**
    - **8.1** Configuring workflows for automated responses to triggers.
- **Practical Exercises (Hands On)**
    - Setting up policies, configuring rules, and generating reports in Falcon.

Implementation Plan:
Each day will include a mix of theoretical learning, live demonstrations, and practical exercises to ensure understanding of CCFA topics and exam readiness.