CrowdStrike University

CERTIFICATION GUIDE

OVERALL PROGRAM DESCRIPTION

CrowdStrike Falcon Certification Program (CFCP) is a multi-tiered certification program, covering three levels of CrowdStrike Falcon users: administrator, front-line analyst and investigator/hunter.

To offer this certification, CrowdStrike draws on a talent pool of seasoned incident responders, investigators/hunters and subject matter experts who use the CrowdStrike Falcon platform daily to perform their incident response duties. This ensures that analysts and administrators who hold one of these certifications have demonstrated a thorough knowledge of the respective areas, and their managers can trust that they can effectively and proficiently use CrowdStrike products and workflows.

Each certification level recommends that the candidate attend the course(s) listed in the Recommended Learning Path for each certification. Although there is no requirement for how recently you completed the recommended learning, candidates are encouraged to stay current on features as the certification is subject to update at any time. Each level of certification also assumes a working knowledge of the tool for that level as well as familiarity with the product guides listed in the Recommended Learning Path.

CROWDSTRIKE CERTIFIED **FALCON ADMINISTRATOR**

Completion of the FHT 100-level courses (or the FHT 200 course) and applicable user guides as listed in the certification description.

CROWDSTRIKE CERTIFIED **FALCON RESPONDER**

Completion of the FHT 201 course and applicable user guides as listed in the certification description. Completion of the FHT 100-level courses is highly recommended.

CROWDSTRIKE CERTIFIED **FALCON HUNTER**

Completion of the FHT 202 course and applicable user guides as listed in the certification description. Completion of FHT 201 and FHT 100-level courses are highly recommended.

CROWDSTRIKE CERTIFIED **FALCON ADMINISTRATOR** (CCFA)

The CCFA certification is directed at the administrator or any analyst with access to the administrative side of Falcon. Examples of positions aligning with this certification are security analyst, security operation center (SOC) analyst, security engineer, IT security operations manager, security administrator, Falcon administrator, and endpoint security administrator.

Persons holding this certification have demonstrated sufficient knowledge to effectively manage the Falcon instance. Specific duties might include: user management and role-based permissions, sensor deployment and management, group creation, deployment and prevention policy settings, allow and block listing, file path exclusion, administrative reporting and more.

This examination is 60 questions and closed book. Candidates are allowed 90 minutes to complete this examination. Candidates who are unsuccessful will receive a second opportunity to complete the examination and should wait 48 hours before the second attempt. Additional information can be found in the CCFA Certification Exam Guide.

Recommended Learning Path: The recommended learning path for CCFA certification is the CSU LP-A: Falcon Administrator Courses. Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Docs:

- Falcon Orientation Guides
- Falcon Sensor Deployment and Maintenance Guides
- Endpoint Security Guides
- User Management Guides
- SEIM Connector Guide

In addition to the above learning path, CrowdStrike suggests that candidates for this certification have at least six months of experience with the CrowdStrike Falcon platform in a production environment.

Tests are administered online through **Pearson VUE.**

It is highly recommended that each participant has a valid subscription to CrowdStrike University.

The cost for each exam is $250 and the voucher can be purchased through your CrowdStrike sales representative or online at Pearson VUE.

Each exam is timed, and candidates will have two opportunities to complete the exam successfully. The passing score for the exam is 80%.

Upon successful completion of the exam, the candidate will receive a score report from Pearson VUE.

Certifications are valid for a period of three years.

Questions regarding Falcon Certification can be sent to **certification@crowdstrike.com**

CROWDSTRIKE CERTIFIED **FALCON RESPONDER** (CCFR)

The CCFR certification is directed at the front-line analyst responding to detections or anyone performing those duties. Examples of positions aligning with this certification are security analyst, SOC analyst, security engineer, IT security operations manager, security administrator and endpoint security administrator.

Persons holding this certification have demonstrated sufficient knowledge to effectively respond to a detection within the Falcon interface and Activity app. Specific duties might include: initial triage of a detection, filtering, grouping, assignment, commenting and status changes. They can conduct basic investigations by performing tasks such as host search, host timeline, process timeline, user search and other click-driven workflows. In addition, they can perform basic proactive hunting for atomic indicators such as domain names, IP addresses, and hash values across enterprise event data, whether the indicator is related to an internal alert or to external intelligence.

This examination is 60 questions and closed book. Candidates are allowed 90 minutes to complete this examination. Candidates who are unsuccessful will receive a second opportunity to complete the examination and should wait 48 hours before the second attempt. Additional information can be found in the CCFR Certification Exam Guide.

Recommended Learning Path: The recommended learning path for CCFR certification is the CSU LP-R: Incident Responder Courses. Completion of FHT 100-level courses in CrowdStrike University is highly recommended. The CCFA certificate is not required,however, it is commonly obtained first, especially for those who perform multiple functions. Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Docs:

- Falcon Orientation Guides
- Endpoint Security Guides
- User Management Guides
- Streaming API Event Dictionary (Review Detection Types)

In addition to the above learning path, CrowdStrike suggests that candidates for this certification have at least six months of experience with the CrowdStrike Falcon platform in a production environment.

CROWDSTRIKE CERTIFIED FALCON HUNTER (CCFH)

The CCFH certification is directed at the investigative analyst who performs deeper detection analysis and response as well as machine timelining and event-related search queries. These analysts are also frequently responsible for insider-threat-related investigations and proactive investigations (hunting) based on intelligence reports and other sources of information. Examples of positions aligning with this certification are hunting team members, security analyst, SOC analyst, security engineer, IT security operations manager, security administrator, and endpoint security administrator.

Persons holding this certification have demonstrated sufficient knowledge to effectively respond to a detection within the Falcon interface and Activity app. They understand which automated reports and queries exist and how to use them to assist in machine auditing and proactive investigation. They have demonstrated the ability to perform simple and intermediate-level search queries using the Splunk syntax. They understand how to navigate between and use multiple views in the Falcon interface such as Process Explorer, Host Search, Host Timeline and Process Timeline to maximize productivity and quickly obtain the desired results.

This examination is 60 questions and closed book. Candidates are allowed 90 minutes to complete this examination. Candidates who are unsuccessful will receive a second opportunity to complete the examination and should wait 48 hours before the second attempt. Additional information can be found in the CCFH Certification Exam Guide.

Recommended Learning Path: The recommended learning path for CCFH certification is the CSU LP-H: Threat Hunter Courses. The CCFA and CCFR certificates are not required, but they may be obtained first, especially for those who perform multiple functions. Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Docs:

- Falcon Orientation Guides
- Endpoint Security Guides
- User Management Guides
- Streaming API Event Dictionary (Review detection types)
- Events Data Dictionary
- Hunting and Investigation Guide

In addition to the above learning path, CrowdStrike suggests that candidates for this certification have at least six months of experience with the CrowdStrike Falcon platform in a production environment.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leverage the cloud-delivered CrowdStrike Falcon Plaform - including next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team - the CrowdStrike services team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

Speak to a representative to learn more about how CrowdStrike Services can help you prepare for and defend against targeted attacks.

CROWDSTRIKE

CROWDSTRIKE
UNIVERSITY