CROWDSTRIKE

CROWDSTRIKE
UNIVERSITY

CERTIFICATION GUIDE

CROWDSTRIKE SERVICES, INC.

LEARN TO STOP BREACHES

Table of Contents

Overall Program Description

The CrowdStrike Falcon Certification Program (CFCP) is a role-based certification program covering different types of CrowdStrike Falcon® users:

- **Falcon Administrators**
- **Falcon Responders** (or front-line SOC analysts)
- **Falcon Hunters** (or forensic investigators)
- **Identity Specialists**
- **Cloud Specialists**

CrowdStrike certification exams are developed in accordance with industry best practices to ensure they are a valid and reliable measure of a candidate's ability to use the Falcon platform for a given job role. Individuals who hold a certification can be trusted to efficiently and proficiently use CrowdStrike products and workflows in their day-to-day activities.

It is strongly recommended that candidates complete the training courses offered in CrowdStrike University that align to each certification. Additionally, candidates should have at least 6 months' experience working in the Falcon platform, as the exam questions measure knowledge and skills gained through hands-on experience.

CrowdStrike Certified Falcon Administrator (CCFA)

CrowdStrike Certified Falcon Responder (CCFR)

CrowdStrike Certified Falcon Hunter (CCFH)

CrowdStrike Certified Identity Specialist (CCIS)

CrowdStrike Certified Cloud Specialist (CCCS)

CrowdStrike Certified Falcon Administrator (CCFA)

The CCFA certification is directed at administrators or any analyst with access to the administrative side of the Falcon platform. Examples of positions aligning with this certification are security analysts, security operations center (SOC) analysts, security engineers, IT security operations managers, security administrators, Falcon administrators and endpoint security administrators.

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, allowlisting and blocklisting, file path exclusion, administrative reporting and more.

This examination has 60 questions and is a closed-book exam. 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 24 hours before the second attempt.

Recommended Learning: It is recommended that candidates complete the Falcon Administrator courses in CrowdStrike University and review the Exam Guide for additional information to help prepare for the certification exam.

Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Documentation:

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

In addition to the above training courses, 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 verifies their access to the learning content available within 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.

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.

Once you pass a Pearson VUE administered exam, you will receive an email with instructions on how to get your digital credentials powered by Credly to share on your social media profiles and how you can download printable certificates for your records.

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

CrowdStrike Certified Falcon Responder (CCFR)

The CCFR certification is directed at front-line analysts responding to detections or anyone performing these duties. Examples of positions aligning with this certification are security analysts, SOC analysts, security engineers, IT security operations managers, security administrators and endpoint security administrators.

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 has 60 questions and is a closed-book exam. 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 24 hours before the second attempt.

Recommended Learning: It is recommended that candidates complete the Falcon Responder courses in CrowdStrike University and review the Exam Guide for additional information to help prepare for the certification exam.

Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Documentation:

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

In addition to the above training courses, 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 investigative analysts who perform 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 analysts, SOC analysts, security engineers, IT security operations managers, security administrators and endpoint security administrators.

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 CrowdStrike Query Language (CQL). 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 has 60 questions and is a closed-book exam. 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 24 hours before the second attempt.

Recommended Learning: It is recommended that candidates complete the Falcon Hunter courses in CrowdStrike University and review the Exam Guide for additional information to help prepare for the certification exam.

Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Documentation:

- 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 training courses, 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 Identity Specialist (CCIS)

The CCIS certification is directed at those working in identity and access management (IAM), analysts focusing on identity-based threats, and policy and access administrators. Examples of positions aligning with this certification are identity managers, analysts, threat hunters and investigators, and Falcon administrators.

The CCIS exam evaluates a candidate's knowledge, skills and abilities to manage domain security with identity-based solutions, administer policy rules and actions, automate responses to identity threats, and manage risk across the authentication landscape in the domain.

A successful CCIS candidate manages identity-based risk in the domain, assesses user and entity risks, investigates identity-based incidents and detections, manages third-party MFA and IDaaS connectors, implements and tunes policies to manage identity-based risks, and maintains the overall identity-based security posture in the domain.

This examination has 60 questions and is a closed-book exam. 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 24 hours before the second attempt.

Recommended Learning: It is recommended that candidates complete the Identity Specialist courses in CrowdStrike University and review the Exam Guide for additional information to help prepare for the certification exam.

Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Documentation:

- Identity Protection Overview
- Identity-Based Incidents, Detections, and Risks
- Identity Protection Reports
- Identity Protection System Notifications
- Identity Protection Insights
- Identity Protection Threat Hunter
- Identity Protection Administration
- Identity Protection Policy
- Identity Protection in Falcon Fusion Workflows
- Integrating Identity Protection with AD FS
- Integrating Identity Protection with PingFederate
- Identity Protection APIs
- Zero Trust Assessment

In addition to the above training courses, 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 Cloud Specialist (CCCS)

The CCCS certification is directed at cloud security engineers who manage the security of their organization's cloud infrastructure. These engineers review the assets, workloads and containers within a cloud environment to see if there are any risky configurations or behaviors that could lead to a breach, and recommend remediations to fix those vulnerabilities. Examples of positions aligning with this certification are cloud security analysts, cloud security engineers, cloud security administrators and cloud security architects.

Persons holding this certification have demonstrated sufficient knowledge to effectively find security gaps in an organization's cloud infrastructure that can be exploited by an adversary. Specific duties might include managing cloud users and role-based permissions; container sensor deployment and management; investigating a finding for a cloud asset, image or container; determining compliance with industry standards; and recommending remediations to fix vulnerabilities.

This examination has 60 questions and is a closed-book exam. 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 24 hours before the second attempt.

Recommended Learning: It is recommended that candidates complete the Cloud Specialist courses in CrowdStrike University and review the Exam Guide for additional information to help prepare for the certification exam.

Candidates should be familiar with the following guides, which are available via the Falcon console by accessing Support > Documentation:

- Cloud Security Overview
- Cloud Security Posture Management: Cloud Asset Inventory and Visualization
- Cloud Security Posture Management: CSPM Automated Remediation
- Cloud Security Posture Management: Configuring CSPM
- Cloud Security Posture Management: Identity Analyzer
- Cloud Security Posture Management: CSPM Overview
- Cloud Security Posture Management: Monitoring CSPM Assessment Findings
- Cloud Security Posture Management: Troubleshooting Cloud Security Posture Management
- Registering Accounts
- Kubernetes and Containers: Container Security
- Kubernetes and Containers: Kubernetes Protection

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