CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFP Certification Exam Guide

Description

The CrowdStrike Certified Falcon Practitioner (CCFP) exam is the final step toward the completion of the CCFP certification. This exam validates foundational knowledge of core cybersecurity concepts and entry-level proficiency with the CrowdStrike Falcon® platform, with a focus on the security operations center (SOC).

A successful CrowdStrike Certified Falcon Practitioner:

- Understands common threat types, basic MITRE ATT&CK® framework concepts, and key security technologies such as endpoint detection and response (EDR), next-gen antivirus (NGAV), extended detection and response (XDR), and security information and event management (SIEM)
- Can describe Falcon's cloud-native architecture, core modules, and the phases of Falcon adoption and how security outcomes evolve across each stage
- Navigates the Falcon console, including menu items, bookmarks, and universal search
- Understands the workflow of an investigation and the key fundamentals of detection, investigation, and response
- Can define how CrowdStrike's threat intelligence enhances the Falcon platform and supports proactive defense, improving operational efficiency by reducing time between detection, response, and remediation
- Understands AI's dual role in cybersecurity as both a threat enabler and a defensive tool and can describe how CrowdStrike Charlotte AI™ and AI-assisted capabilities within the Falcon platform accelerate analyst workflows and support responsible security operations

Additionally, it is recommended that the candidate has three (3) to six (6) months of experience working in the CrowdStrike Falcon platform.

CrowdStrike Certification Program

Requirements

All exam registrants must (no exceptions):

- Accept the CrowdStrike Certification Exam Agreement
- Be at least 18 years of age
- Purchase a CrowdStrike exam voucher to register for the exam

Contact your CrowdStrike Account Executive to request a quote or purchase a CrowdStrike exam voucher through Pearson.

Learning Access

It is **strongly recommended** that all exam candidates have access to CrowdStrike University and confirm they can view available learning options associated with their CrowdStrike University account.

- CrowdStrike certification-aligned courses are available to learners with an active CrowdStrike University account.
- A unique CrowdStrike Certification ID, training transcripts, and printable certification documents are available through the CrowdStrike University learning management system.

NOTE: All exam takers can view and print their CrowdStrike certification exam score report through Pearson.

Recommended Certification Candidate Competence and Abilities

- Candidates should have three (3) to six (6) months of experience with CrowdStrike Falcon in a production environment.
- Candidates should read English with sufficient accuracy and fluency to support comprehension. Exams are suitable for non-native English speakers.

About the Exam

Assessment Method

The CCFP exam is a 90-minute, 60-question assessment.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCFP certification exam
- Refrain from any misconduct

In the event of misconduct by the candidate, CrowdStrike may invalidate the score and consider any suspicious action a violation of the CrowdStrike Certification Exam Agreement.

When a candidate has completed the exam and the candidate's official exam score has been posted, the certification candidate may view the official exam score through Pearson.

Retake Policy

Candidates who do not pass an exam on their first attempt:

- Must wait 48 hours to retake the exam (wait time begins after the exam)
- Should review the exam objectives, training course materials, and associated recommended reading listed in this document

After the second attempt, a candidate will need to wait seven (7) days for the third attempt and any subsequent attempts. Wait time begins the day after the attempt.

Candidates who want to retake the exam should consider retaking the applicable recommended course(s) and gain additional experience with the CrowdStrike Falcon platform before trying again.

Retakes beyond the fourth attempt will be considered on a case-by-case basis. CrowdStrike reserves the right to deny a retake beyond the fourth attempt. If the fourth attempt is a failure due to a technical issue, the candidate can reattempt the exam a fifth time.

If the candidate fails for a fourth time due to personal performance, they must wait 30 days and retake the recommended training indicated in the exam guide. CrowdStrike will verify that the candidate has retaken the recommended training in the exam guide and has met with the CrowdStrike Certification Manager before they are cleared to register for a fifth exam attempt.

Retaking Previously Passed Exams

Candidates will not be permitted to retake any exam they have previously passed unless directly related to a recertification requirement approved by CrowdStrike.

Beta Exams

Candidates will not be permitted to retake beta exams.

Exam Challenge

If a certification candidate believes there is an error on an exam or that specific questions on the CCFP exam are invalid, contact certification@crowdstrike.com to submit an evaluation request. The certification candidate must submit a claim within three (3) days of taking the exam for it to be considered. CrowdStrike will generally respond to a submission within fifteen (15) business days.

Recertification

All CrowdStrike certifications are valid for three (3) years from the date of successful completion of an exam. Recertification requires passing the most current version of the exam upon expiration of certification.

Exam Preparation

Recommended Learning

CrowdStrike strongly recommends certification candidates complete the CrowdStrike Certified Falcon Practitioner courses in CrowdStrike University to prepare for the CCFP exam. To learn more about these courses, view the CrowdStrike Training Catalog.

It is also recommended that candidates are familiar with the following guides, which are available via the Falcon console by accessing Support and resources > Documentation portal:

- Falcon Platform Overview / Getting Started Guide
- Falcon Insight XDR Documentation
- Threat Intelligence Documentation
- Charlotte AI Documentation
- Endpoint Security / Prevention Policy Documentation

Exam Scope

The following topics provide a general guideline for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam.

1. Cybersecurity Fundamentals
2. Falcon Platform Overview
3. Core Operational Workflows
4. AI and Automation in Falcon

Scope Changes

To better reflect the content of the exam and for clarity purposes, the following guidelines may change at any time without notice. Such changes may include, without limitation, adding or deleting an available CrowdStrike certification; modifying certification requirements; and making changes to recommended training courses, testing objectives, outline, and exams, including, without limitation, how and when exam scores are issued. The certification candidate agrees to meet (and continue to meet) the program requirements, as amended, as a condition of obtaining and maintaining the certification.

Exam Objectives

The following subtopics and learning objectives provide further guidance on the content and purpose of the exam:

1. Cybersecurity Fundamentals

1.1 Identify and differentiate between common threat types encountered in modern SOC environments (malware, ransomware, phishing, lateral movement)

1.2 Identify the core components of the MITRE ATT&CK framework, including the difference between tactics and techniques

1.3 Define and differentiate core security concepts (EDR, NGAV, XDR, SIEM, Cloud) and their roles in an organization's security architecture

1.4 Understand how cybersecurity concepts translate into day-to-day SOC work, including the typical SOC analyst workflow, alert fatigue, triage prioritization, and dwell time

1.5 Understand different architectures (e.g., single-tenant vs. multi-tenant) and how these impact detections and preventions

1.6 Understand AI's role in cybersecurity as both a threat enabler (allowing adversaries to move swiftly) and a defensive tool (to detect threats and automate response)

2. Falcon Platform Overview

2.1 Articulate the key architectural principles of the Falcon platform (cloud-native model, lightweight sensor, single console, multi-tenant, and dwell time)

2.2 Identify and describe the primary Falcon modules and their purpose at a high level (Falcon Prevent, Falcon Insight XDR, Falcon Exposure Management, Falcon Next-Gen Identity Security, Falcon Next-Gen SIEM, Falcon Cloud Security, Falcon AIDR, Charlotte AI)

2.3 Describe the phases of Falcon adoption and explain how security outcomes evolve across each stage, from initial visibility through detection, investigation, response, and operationalization

2.4 Articulate how threat intelligence enhances the Falcon platform (adversary intelligence, indicator enrichment, proactive defense, integration within Falcon)

2.5 Explain the operational benefits of the Falcon platform (reduced alert fatigue, acceleration of detection and response times, increased automation capabilities)

3. Core Operational Workflows

3.1 Navigate the Falcon console to locate and access key features (e.g., menu items, bookmarks, universal search)

3.2 Understand how Falcon surfaces threats through detections and alerts, including how they are prioritized and what information they provide to security teams (e.g., MITRE, Falcon Detection Language, detection-based context and operations)

3.3 Describe the steps of a basic investigation flow within the Falcon platform

3.4 Understand the relationship between detection, investigation, and response as a continuous cycle

4. AI and Automation in Falcon

4.1 Understand the role of AI across the Falcon platform (e.g., Charlotte AI, Falcon AIDR, agentic workflows, machine learning within CrowdStrike Threat Graph)

4.2 Understand Charlotte AI's role and capabilities, including use cases and how AI-assisted triage accelerates analyst workflows

4.3 Understand responsible AI in security, including benefits and risks of integrating AI into the security workflow

CROWDSTRIKE UNIVERSITY