



CROWDSTRIKE
UNIVERSITY

TRAINING CATALOG

CROWDSTRIKE SERVICES, INC.

LEARN TO STOP BREACHES

Table of Contents

Overview and Basic Information	3
Falcon Platform	6
Endpoint Security	10
Cloud Security	15
Identity Protection	19
Data Protection	21
Threat Intelligence	23
IT and Security Operations	26
Observability and Log Management	28

Overview and Basic Information

OVERVIEW

Take full advantage of all that the CrowdStrike Falcon® platform has to offer with CrowdStrike's industry-leading training and certification. Learn what you need to know to get started with the Falcon platform, gain advanced skills to use on the job and take exams to become a CrowdStrike certified professional. At CrowdStrike University, there is a learning path and certification for you. With the right training, anyone can harness the power of the Falcon platform.

CROWDSTRIKE UNIVERSITY

CrowdStrike University is an online learning management system (LMS) that organizes all CrowdStrike eLearning, instructor-led training and certification in one place, providing a personalized learning experience for individuals who have an active training subscription.

Fundamental cybersecurity knowledge and training is provided through a training subscription to CrowdStrike University. This per-learner training subscription provides access to self-paced eLearning courses, "What's New in Falcon" videos (WNIFs), the global training calendar and the online portal for taking CrowdStrike certification exams. Through CrowdStrike University, you can access:

- **Self-paced courses:** Disseminating fundamental cybersecurity knowledge and skills, CrowdStrike eLearning courses are divided into modules so you can stop and start as needed or jump to a specific topic.
- **"What's New in Falcon" videos (WNIFs):** Learn about the latest updates to CrowdStrike products, new and updated features, and other timely topics through short training videos.
- **Quick technical tips (QTTs):** Access quick technical tips for the most common problems with this how-to video series.
- **Instructor-led training (ILT):** With the purchase of CrowdStrike training credits, you can view and register for upcoming live sessions to gain knowledge and skills from CrowdStrike experts and practice in the cloud-based Falcon platform training lab.
- **CrowdStrike certification:** With the purchase of exam vouchers, you can register for and take CrowdStrike certification exams through Pearson VUE, CrowdStrike's test delivery vendor.

ACCESSING CROWDSTRIKE UNIVERSITY

Access is provided via a training subscription to named learners with:

- **An LMS Annual Subscription** (requires purchase) OR
- **A Customer Access Pass** — Organizations may be eligible for a specified number of free customer access passes based on contract eligibility. To find out if your organization may qualify, see the [Customer Access Pass](#) data sheet.

Learners with an active LMS annual subscription or Customer Access Pass have full access to CrowdStrike University's self-paced training library, including eLearning fundamentals courses, WNIF videos and QTTs. CrowdStrike training subscriptions are transferable with documented change of staff — limited to 10% of subscriptions purchased per year.

Learners who want to take ILT classes must have an active CrowdStrike University account, and the learner's organization must purchase CrowdStrike training credits that are applied to instructor-led class sessions.

Learners who wish to take a CrowdStrike certification exam are strongly advised to have an active CrowdStrike University account. The learner's organization must purchase CrowdStrike exam vouchers that are applied to certification exam requests. Certification exams are delivered by Pearson VUE and can be taken online or at a Pearson VUE testing center. Learners can schedule their exam at [PearsonVue/CrowdStrike](#).

Contact your account executive to purchase CrowdStrike University training subscriptions, training credits and exam vouchers. If you have a training subscription and need access to CrowdStrike University, contact your technical account manager for assistance or email LMS-Helpdesk@crowdstrike.com.

TRAINING DELIVERY

Choose from a range of flexible options, including:

- Self-paced eLearning
- Regional in-person classroom instructor-led training
- Live online instructor-led training (using remote meeting technology)
- Private onsite instructor-led training (delivered at your organization's site)
- Private live online instructor-led training

Live online training

Live online class sessions are delivered through Zoom remote conferencing technology. For the best learning experience, CrowdStrike suggests that learners have the following:

- Dual monitors
- Headset with microphone
- Quiet place to attend sessions

Requirements for onsite training

Onsite training delivery requires:

- At least three consecutive days of training (any courses)
- A minimum of 10 students for each day
- A surcharge of eight (8) training credits for domestic travel (within the continental United States) or sixteen (16) training credits for international travel per week

Requirements for private classes

Both live online and onsite private instructor-led training classes have a 10-student minimum and a 15-student maximum per class/day of instruction.

Scheduling

Private and onsite training can be scheduled by contacting training@crowdstrike.com.

CROWDSTRIKE UNIVERSITY COURSES

CrowdStrike offers a robust catalog of classes with convenient options to help learners keep their knowledge current and practice new skills, empowering them to better protect your organization and stop breaches. Self-paced eLearning and instructor-led training courses are available through CrowdStrike University. Courses may be added, modified or removed from this training catalog document; for the latest course list, sign in to CrowdStrike University and view the Content Library.

SELF-PACED eLEARNING COURSES

Take digital courses on demand at the time and pace that is most convenient for you. CrowdStrike's self-paced courses are designed with interactivity in mind. All eLearning courses labeled with a FALCON prefix have been updated to reflect the recent Raptor changes in the Falcon platform.

INSTRUCTOR-LED TRAINING COURSES

Through CrowdStrike University, cybersecurity professionals can take advantage of instructor-led training across multiple days and time zones around the globe. Engage with CrowdStrike experts and fellow students live, and practice what you learn in class in the cloud-based Falcon lab environment. See the [CrowdStrike training calendar](#) for upcoming events hosted by CrowdStrike. All instructor-led training courses require each learner to have an LMS Annual Subscription or a Customer Access Pass to CrowdStrike University.

CROWDSTRIKE FALCON CERTIFICATION PROGRAM

The [CrowdStrike Falcon Certification Program](#) (CFCP) aligns certifications to the job roles of users, from Falcon platform administrators and front-line analysts/incident responders to proactive investigators/hunters and specialists for cloud security and identity protection. Certifications are developed by analyzing the skills, knowledge and abilities of subject matter experts who use the Falcon platform daily to ensure professionals who hold certifications have demonstrated proficient use of the Falcon platform.

Available certifications include:

- [CrowdStrike Certified Falcon Administrator \(CCFA\)](#)
- [CrowdStrike Certified Falcon Responder \(CCFR\)](#)
- [CrowdStrike Certified Falcon Hunter \(CCFH\)](#)
- [CrowdStrike Certified Identity Specialist \(CCIS\)](#)
- [CrowdStrike Certified Cloud Specialist \(CCCS\)](#)

Certification candidates can take CrowdStrike certification exams through the global network of Pearson VUE test centers or take the exam online using Pearson's OnVUE testing service. The cost for each exam is one (1) exam voucher; candidates will have two (2) opportunities to pass the exam successfully. Exams are time-based. Upon successful completion of an exam, the candidate will receive a score report. Certifications are valid for a period of three (3) years.

The background features a series of concentric, curved lines in a dark red color, creating a sense of depth and movement. The lines are more densely packed on the left side and become more widely spaced towards the right. The overall color palette is a gradient of reds, from a deep, dark red to a bright, vibrant red.

Falcon Platform

Self-Paced eLearning

FHT 100: Falcon Platform Architecture Overview

Learn about the unified cloud-native architecture of the Falcon platform, which provides the foundation to defend against modern cyberattacks in an evolving threat landscape. This course will present the basics of the Falcon platform architecture, including the CrowdStrike® Security Cloud, CrowdStrike Threat Graph®, CrowdStrike Falcon® Fusion and the Falcon agent.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 101: Falcon Platform Technical Fundamentals

Join Team Falcon in this high-level overview of the Falcon console. Learners will select their learning path based on their main job responsibilities. This course will provide information for applications in the Falcon console that are relevant to different roles and provide a high-level walkthrough of these applications. Learners will also be provided with additional courses and materials to help them on their heroic journey to save the organization!

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 102: Falcon Platform Onboarding Configuration

Walk through the steps to setting up the Falcon platform in your environment through this interactive scenario-based challenge.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 104: Getting Started with the Endpoint Security Module

This endpoint security course shows you how to monitor, review and respond to detections in your environment. In this course, learners will walk through various aspects of endpoint security.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 105: Sensor Installation, Configuration and Troubleshooting

Understand what to consider during the pre-installation phase of a Falcon sensor, see installation examples and options, learn how to install a sensor and get troubleshooting tips for common installation issues.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 106: Customizable Dashboards

Falcon customizable dashboards help users see preconfigured views of commonly useful detection data. Users will learn to surface specific details or summarize unique combinations of information for your organization's needs. Users will also learn to create their own customized dashboards to use privately or share with other users in their organization.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 114: Falcon Fusion Fundamentals

Falcon Fusion is a unified and extensible framework purpose-built on the CrowdStrike Falcon platform to orchestrate and automate simple and complex workflows. In this brief course, you will learn how you can use this workflow builder to define how you want the Falcon platform to respond to certain triggers, such as incidents, detections, cloud security findings, updates made by users and more.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 115: Create a Falcon Fusion Workflow

Hack Attack discovered that Team Falcon is short-staffed and thinks this is the prime time to infiltrate the organization! Help the responder stop the adversary by learning how to create Falcon Fusion workflows. You can use Falcon Fusion to create workflows that allow you to respond more quickly to critical issues. This course will walk you through creating a complex workflow step by step.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 176: Understanding the Basics of PSFalcon

This course introduces the CrowdStrike API SDK for PowerShell, also known as PSFalcon. Learn how to install PSFalcon locally on various endpoints and generate an API client, examine PSFalcon commands to pull relevant and filtered data from the API, and review common PSFalcon use cases and sample scripts.

- Format: Self-paced eLearning
- Duration: 60 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CQL 101: CrowdStrike Query Language Fundamentals 1

This brief course introduces learners to the CrowdStrike Query Language. Participants will learn essential concepts, techniques and best practices to create effective and efficient CQL queries. The course will cover basic topics, allowing participants to develop their skills in writing CQL query statements.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

FALCON 200: Falcon Platform for Administrators

Learn technical fundamentals of the Falcon platform. This course is appropriate for new platform users and focuses on installation, configuration and day-to-day management. A complete console walkthrough and hands-on labs are included.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [FALCON 200: Course Syllabus](#)

Certification

CrowdStrike Certified Falcon Administrator (CCFA)

This exam evaluates the candidate's knowledge and skills in managing various components of the Falcon platform on a daily basis, including sensor installation.

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: [Infographic](#)

Follow the recommended [Falcon Administrator Learning Path](#) in CrowdStrike University to prepare for CCFA certification.





Endpoint Security

Self-Paced eLearning

FALCON 104: Getting Started with the Endpoint Security Module

This endpoint security course shows you how to monitor, review and respond to detections in your environment. In this course, learners will walk through various aspects of endpoint security.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 107: Falcon Firewall Management Fundamentals

Understand the technical foundational skills required to be able to add, manage, enable/disable and delete firewall rules, rule groups and policies.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 108: Reducing USB Device Risk with Falcon Device Control

Many users rely on USB devices to do their jobs every day, exposing organizations to potential risks such as malware or loss of sensitive information. Some organizations choose to block all USB devices, but this can impede employee productivity. CrowdStrike Falcon® Device Control provides visibility, blocking and granular control over the device connections in an organization. This course will review Falcon Device Control and enable you to create device policies that can reduce USB device risks.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 109: Using MITRE ATT&CK and Falcon Detection Methods to Understand Security Risk

Learn about the MITRE ATT&CK® framework and CrowdStrike's implementation of that framework.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 120: Investigation Fundamentals

Learn how to investigate a potential compromise using the Falcon platform. This course covers the types of data the Falcon platform captures, how to access this data through the Falcon platform and the sections of the Falcon platform that should be used for different investigation types.

- Format: Self-paced eLearning
- Duration: 35 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 124: Discover for IoT Fundamentals

Critical infrastructure systems remain vulnerable to cyberattacks, and organizations need to secure their industrial control system (ICS) in conjunction with the assets contained in their IT and operational technology (OT) systems. CrowdStrike Falcon® Discover for IoT extends security hygiene across ICS, IT and OT environments to address the challenges security teams face. This course will explain how to use the ICS collector to gather information from IT, OT and IoT devices in an environment; navigate to the Falcon Discover for IoT dashboard and other pages; examine IoT asset data; and define key terminology related to Falcon Discover for IoT.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 125: Falcon Flight Control Fundamentals

CrowdStrike Falcon® Flight Control provides cybersecurity management and monitoring for security systems and devices across multiple accounts by arranging customer IDs (CIDs) into a parent/child hierarchy. Through one parent ID, customers can manage separate child CIDs, allowing them to manage policies, respond to detections and manage API access.

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 140: Real Time Response Fundamentals

Learn to use the Falcon Real Time Response (RTR) feature and run incident response commands directly within the Falcon console to respond to detected incidents.

- Format: Self-paced eLearning
- Duration: 60 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 150: Incidents Fundamentals

Learn the fundamentals of Activity > Incidents. Participants will learn how to work through and edit an incident. This course includes guided walkthroughs and video demonstrations.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 160: Falcon for Mobile Fundamentals

Bring endpoint detection and response to mobile devices. Learn how CrowdStrike Falcon® for Mobile allows users to view detections and events from your organization's supervised and unsupervised Android and iOS mobile devices.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FHT 180: Falcon Forensics Fundamentals

Learn about CrowdStrike Falcon® Forensics and how to deploy Falcon Forensics using the Falcon RTR feature of CrowdStrike Falcon® Insight XDR and PSFalcon.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

FALCON 201: Falcon Platform for Responders

Learn the best use of the Falcon platform for incident triage. This course is appropriate for incident responders or SOC analysts who use the Falcon platform daily and focuses on triaging and responding to alerts. Hands-on lab exercises are included.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [FALCON 201: Course Syllabus](#)

FALCON 202: Investigating and Querying Event Data with Falcon EDR

Learn the best use of the Falcon platform for incident detection using proactive investigation techniques. The course is appropriate for those who use the Falcon platform to find evidence of incidents that did not raise alerts by other means and includes practical labs for students to develop hands-on skills.

Please note: This course is based on the product features introduced with the Raptor release in September 2023. If you need a course based on pre-Raptor content, please register for [FHT 202: Investigating and Querying Event Data With Falcon EDR](#).

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [FALCON 202: Course Syllabus](#)

FALCON 240: Investigating and Mitigating Threats with Real Time Response

Falcon Real Time Response is used for remediation, host-level responses to detections and host investigations. In this course, you will use Real Time Response to query information from hosts, put and run files and scripts, and remotely perform the tasks that a responder would perform if they were physically present at an endpoint.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [FALCON 240: Course Syllabus](#)

FHT 280: Investigating with Falcon Forensics

Learn how to conduct investigations and threat hunt using Falcon Forensics dashboards and Splunk searches. This course is intended for threat hunters who will utilize Falcon Forensics to collect forensic information and use that information to perform investigations. Hands-on lab exercises are included.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [FHT 280: Course Syllabus](#)

FALCON 302: Advanced Threat Hunting with Falcon

Utilizing the CrowdStrike Falcon platform, participants will learn to hunt for signs of an adversarial compromise. This course focuses on finding abnormal enterprise activity and searching for related data points, with the goals of finding all impacted hosts and – when possible – identifying the adversary. Students will learn advanced threat hunting techniques to use throughout the entire threat hunting cycle. Topics include initiating hunts, developing search techniques and reporting findings. The course delves into in-depth investigation of Falcon events, application of common threat models and the use of structured analysis to bridge knowledge gaps.

- Format: Instructor-led training
- Duration: 3 days | 24 hours
- Cost: 6 training credits
- Learn More: [FALCON 302: Course Syllabus](#)

Certification

CrowdStrike Certified Falcon Responder (CCFR)

This exam evaluates the candidate's knowledge and skills when responding to a detection within the Falcon console and Activity app.

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: [Infographic](#)

Follow the recommended [Incident Responder Learning Path](#) in CrowdStrike University to prepare for CCFR certification.



CrowdStrike Certified Falcon Hunter (CCFH)

This exam evaluates the candidate's knowledge and skills when responding to a detection within the Falcon console and Activity app and when using reports and queries to assist in machine auditing and proactive investigation.

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: [Infographic](#)

Follow the recommended [Threat Hunter Learning Path](#) in CrowdStrike University to prepare for CCFH certification.





Cloud Security

Self-Paced eLearning

CLOUD 100: Falcon Cloud Security Fundamentals

The majority of cloud breaches are due to human error. These errors might stem from leaving workloads and containers open to the public or from not restricting access to accounts or APIs. What can organizations do? In this brief course, you will see an overview of some basic cloud concepts and get information on how the Falcon platform can help protect your cloud assets.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 123: Cloud Security Posture Fundamentals

In this course, you will learn how the Falcon Cloud Security posture management and cloud infrastructure entitlement management (CIEM) Identity Analyzer can help you keep your cloud configurations secure and follow industry cloud security recommendations. Find recommended remediations so you can address potential threats in your cloud environment such as misconfigurations, exposed cloud assets and over-privileged cloud accounts.

- Format: Self-paced eLearning
- Duration: 55 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 124: Cloud Security Posture Management (CSPM) Registration and Configuration

In this course, you will learn how to set up your cloud accounts for AWS, Azure and GCP so you can get started with CSPM in the CrowdStrike Falcon Cloud Security module. Get a brief overview on how to configure policies and discover different ways to operationalize CSPM to meet your organization's security needs.

- Format: Self-paced eLearning
- Duration: 26 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 171: CrowdStrike Container Security and Image Assessment

CrowdStrike Falcon® Cloud Security: Container Security delivers complete security and compliance for cloud-native applications and solves many common challenges developers and system administrators face, such as vulnerable images or apps, cross-container attacks, container breaks and privileged escalations. This course will guide learners through the steps needed to create or push images for assessment, how to secure Kubernetes in the Falcon container sensor, and how to view and analyze the data in the dashboards.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 172: Setting Up Cloud Workload Protection (CWP) with Falcon Cloud Security

In this course, you will learn about the different Kubernetes agent and Falcon sensor deployment solutions available for CrowdStrike Falcon® Cloud Security for Containers. Get a brief overview of these deployment solutions, which are best for your environment, and how to install and deploy these agents and sensors at a high level.

- Format: Self-paced eLearning
- Duration: 10 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 190: Save the Cloud!

Join CrowdStrike Counter Adversary Operations and The Responder from Team Falcon as they work to prevent a massive adversary breach in a cloud environment. Learn a few best practices for protecting your cloud assets using CrowdStrike cloud security products and other security tools by reviewing hypothetical scenarios and choosing from several possible answers.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CLOUD 191: Falcon Cloud Security Activity Dashboard

The Cloud Security Activity dashboard allows users of CrowdStrike Falcon® Cloud Security to monitor the high-level security status of their entire cloud environment through one pane of glass. In this brief course, you will walk through the data available on the dashboard and see suggestions for how the dashboard can be used to prioritize and remediate top cloud security issues.

- Format: Self-paced eLearning
- Duration: 10 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

CLOUD 223: Identifying Risks in Your Cloud Environment with CSPM

Learn how to use CrowdStrike Falcon Cloud Security's CSPM to secure cloud environment configurations and remain in compliance with industry standards. Find out how CSPM can help you determine if any of your cloud assets are misconfigured, if you are meeting your industry standards for security and if any behaviors affecting your cloud assets are malicious. You will also learn to locate cloud accounts with vulnerabilities, find the steps to remediate them and learn where to communicate those findings.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [CLOUD 223: Course Syllabus](#)

CLOUD 271: Securing Cloud Workloads and Containers with Falcon Cloud Security

The complexity of public and private cloud infrastructure requires development teams to incorporate security into all aspects of the development life cycle. In this course, you will learn how to use Falcon Cloud Security and “shift left” to protect containerized workloads and cloud-native applications.

This course includes security best practices and tips for using Falcon Cloud Security to mitigate common threats to cloud workloads. You will learn to proactively identify common threats and mitigate risks at every stage of application development. Learn how to avoid the financial and reputational costs of breaches to your organization and improve your overall security posture.

- Format: Instructor-led training
- Duration: 1 day
- Cost: 2 training credits
- Learn More: [CLOUD 271: Course Syllabus](#)

Certification

CrowdStrike Certified Cloud Specialist (CCCS)

The CrowdStrike Certified Cloud Specialist (CCCS) exam is the final step toward the completion of CCCS certification.

This exam validates a candidate's knowledge, skills and abilities when performing the dual role of administrator and vulnerability manager in the Falcon platform. Successful candidates are proficient in setting up and configuring Falcon Cloud Security and monitoring and mitigating security issues in an organization's cloud environment.

- Exam Questions: 60
- Duration: 90 minutes

Follow the recommended [Cloud Specialist Learning Path](#) in CrowdStrike University to prepare for CCCS certification.



Identity Protection

Self-Paced eLearning

IDP 170: Falcon Identity Protection Fundamentals

Participants will learn about CrowdStrike Falcon® Identity Protection and ways to gain value beyond initial deployment. In this course, you will learn about key components of the CrowdStrike Falcon® Identity Threat Detection and CrowdStrike Falcon® Identity Threat Protection modules, the installation and deployment process, visibility and detection use cases, Zero Trust use cases and policy management basics.

- Format: Self-paced eLearning
- Duration: 60 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

IDP 172: Zero Trust Fundamentals

This course consists of a series of micro-videos describing the three stages of the Zero Trust journey, best practices for each stage and quick tips on how to leverage the Falcon platform at each stage. This course also includes an interactive walkthrough of the CrowdStrike Falcon® Zero Trust Assessment (ZTA) dashboard and a short demo highlighting a Zero Trust use case.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

IDP 270: Securing Workforce Identities with Falcon Identity Protection

This course will cover the Falcon Identity Protection modules and demonstrate how to configure, implement and utilize the data feeds from Falcon Identity Protection to secure your workforce identities. Whether you want to monitor for weak or compromised passwords, analyze stale or stealthy administrators in your domain, or enforce multifactor authentication (MFA) for high-risk users, this course will provide you with the tools you need to leverage the Falcon Identity Protection tool set and lock down your domain.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [IDP 270: Course Syllabus](#)

Certification

CrowdStrike Certified Identity Specialist (CCIS)

The CrowdStrike Certified Identity Specialist (CCIS) exam validates a candidate's knowledge, skills and abilities to perform as an Identity Specialist within an organization using Falcon Identity Protection.

A successful CrowdStrike Certified Identity Specialist 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.

- Exam Questions: 60
- Duration: 90 minutes

Follow the recommended [Identity Specialist Learning Path](#) in CrowdStrike University to prepare for CCIS certification.



Data Protection

Self-Paced eLearning

FALCON 190: Falcon Data Protection Fundamentals

This course provides learners with the knowledge to leverage the advanced visibility, classification and policy management options available in the CrowdStrike Falcon® Data Protection module to protect critical assets from unauthorized egress through supported channels.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass



Threat Intelligence

Self-Paced eLearning

CTI 130: CrowdStrike Falcon Intelligence Fundamentals

Learn the fundamentals of CrowdStrike Falcon® Intelligence, including adversary intelligence, reports, threat actors, tailored intelligence and API integrations. Learn to submit requests for information (RFIs) and malware for analysis and summary recommendations.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CTI 131: CrowdStrike Falcon Sandbox Fundamentals

CrowdStrike Falcon® Sandbox is the most advanced and powerful malware sandbox available. This course will show you how to investigate, submit and analyze files to protect your organization from malicious threats.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CTI 132: CrowdStrike Falcon Intelligence Recon Fundamentals

Learn the fundamentals of CrowdStrike Falcon® Intelligence Recon, including how to search and view search results and set up monitoring rules and notifications.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CTI 142: Falcon MalQuery Fundamentals

CrowdStrike Falcon® MalQuery is the leading malware research tool in the industry. Its efficient, patent-pending indexing technology and robust search algorithms allow for intricate hunting throughout years' worth of malware samples. This course covers the key benefits of Falcon MalQuery along with the basics of searching, hunting and monitoring with Falcon MalQuery.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

CTI 330: Creating Intelligence with CrowdStrike Falcon

Learn the doctrinal concepts of gathering and analyzing information to create intelligence products and about cyber threat intelligence methodologies. This course is appropriate for managers, report writers, intelligence consumers and analysts of all types who have minimal experience in intelligence functions and production. Hands-on lab exercises are included.

- Format: **Private class only**
- Duration: 2 days | 16 hours
- Cost: 4 training credits
- Learn More: [CTI 330: Course Syllabus](#)

Please contact training@crowdstrike.com or your account manager for more details on this class.

CTI 346: Structured Analytic Techniques for Cyber Analysts

Structured analytic techniques are scientifically derived tools used by analysts to abstract biases out of analyses and gain insight into the meaning and value of large sets of information. Use these techniques to provide better accuracy, relevancy and substance to intelligence reporting. Learn the five core categories of structured analysis and practice with dozens of trusted analytic tools. Hands-on lab exercises are included.

- Format: **Private class only**
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [CTI 346: Course Syllabus](#)

Please contact training@crowdstrike.com or your account manager for more details on this class.



IT and Security Operations

Self-Paced eLearning

ITSEC 120: Falcon Exposure Management Fundamentals

CrowdStrike Falcon® Exposure Management is a new product offering that consists of several existing CrowdStrike modules – including CrowdStrike Falcon® Spotlight, CrowdStrike Falcon® Discover and CrowdStrike® Falcon Surface™ – and expands upon them with additional features that are only available through Falcon Exposure Management. This course will explain the benefits of Exposure Management and how it can help you get visibility into your assets and uncover vulnerabilities. Get an overview of Falcon Exposure Management and learn about the requirements for using Falcon Exposure Management, Falcon Exposure Management tools, exposure dashboards, active discovery, asset criticality rules, internet exposure paths using CrowdStrike® Asset Graph™ and configuration assessment.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

ITSEC 121: Falcon Spotlight Fundamentals

Falcon Spotlight is a scanless endpoint vulnerability management module that allows you to view the vulnerabilities that exist in your environment. The integration of vulnerability management into the Falcon platform allows you to take advantage of excellent endpoint security and get vulnerability visibility. This course will explain the benefits of Falcon Spotlight, how it helps reduce the risk of a breach and how to use Falcon Spotlight effectively.

- Format: Self-paced eLearning
- Duration: 40 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

ITSEC 122: Falcon Discover Fundamentals

Falcon Discover is CrowdStrike's IT hygiene module. Falcon Discover allows you to get real-time visibility into who and what is in your network. In this course, you will get an overview of Falcon Discover and understand how to better manage the assets, accounts and applications running in your environment.

- Format: Self-paced eLearning
- Duration: 40 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

ITSEC 126: Falcon FileVantage Fundamentals

CrowdStrike Falcon® FileVantage is a file integrity monitoring module. It simplifies the security stack and provides real-time insight for file changes, offering valuable contextual data for detections.

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

ITSEC 128: Falcon Surface Fundamentals

Falcon Surface is an external attack surface management (EASM) solution. With Falcon Surface, you can manage your external attack surface by detecting, prioritizing and managing your internet-facing assets; see prioritized security issues; and resolve risks with generated remediation advice. This course will explain the benefits of Falcon Surface and how to use Falcon Surface effectively.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass



Observability and Log Management

Self-Paced eLearning

Before Getting Started with Falcon LogScale

It is recommended that learners have completed FALCON 100, FALCON 101 and CQL 100 before starting the LOG 101 and LOG 165 courses. This will provide the necessary foundation you need for the Falcon platform and CrowdStrike Query Language.

FHT 100: Falcon Platform Architecture Overview

Learn about the unified cloud-native architecture of the Falcon platform, which provides the foundation to defend against modern cyberattacks in an evolving threat landscape. This course will present the basics of the Falcon platform architecture, including the CrowdStrike® Security Cloud, CrowdStrike Threat Graph®, CrowdStrike Falcon® Fusion and the Falcon agent.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

FALCON 101: Falcon Platform Technical Fundamentals

Join Team Falcon in this high-level overview of the Falcon console. Learners will select their learning path based on their main job responsibilities. This course will provide information for applications in the Falcon console that are relevant to different roles and provide a high-level walkthrough of these applications. Learners will also be provided with additional courses and materials to help them on their heroic journey to save the organization!

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

CQL 101: CrowdStrike Query Language Fundamentals 1

This brief course introduces learners to the CrowdStrike Query Language. Participants will learn essential concepts, techniques and best practices to create effective and efficient CQL queries. The course will cover basic topics, allowing participants to develop their skills in writing CQL query statements.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

LOG 101: Getting Started with Falcon LogScale

The flexible, modern architecture of CrowdStrike® Falcon LogScale™ improves and enhances the log management experience for organizations by enabling complete observability to answer any question, explore threats and vulnerabilities, and gain valuable insights from all logins in real time. In this series of videos, participants will be introduced to Falcon LogScale log management. They will learn about foundational concepts such as navigating the user interface, ingesting data into Falcon LogScale, dashboard creation, turning live or streaming queries into real-time alerts and programmatic ways to interact with Falcon LogScale.

- Format: Self-paced eLearning
- Duration: 60 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

LOG 165: Falcon Long Term Repository Fundamentals

Learn how you can use CrowdStrike Falcon® Long Term Repository to search/mitigate threats and carry out investigations based on historical data. This course includes several videos and interactions that guide you through use cases, the various roles and functions that interface with historical data, how the data comes into the platform and the steps you need to take to work with the data.

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

Instructor-Led Training

LOG 200: Falcon LogScale for Administrators

The Falcon LogScale for Administrators course will teach participants how to configure and maintain the main components of Falcon LogScale in an installed instance. Participants will walk through the steps and techniques used to administer a Falcon LogScale environment and manage authentication and authorization, and they will explore how data gets into Falcon LogScale.

- Format: Instructor-led training
- Duration: 2 days
- Cost: 4 training credits
- Learn More: [LOG 200: Course Syllabus](#)

LOG 201: Preparing, Ingesting and Parsing Log Data Using Falcon LogScale

Does your organization use Falcon LogScale to aggregate and search data from a wide variety of log sources at scale? This course offers a deep dive into preparing, ingesting and parsing datasets using Falcon LogScale. Designed for those who are new to the field or looking to refresh their skills, the course presents techniques for data cleaning, dimensional reduction, normalization and statistical interpretation. Delve into key data analysis terminology, familiarize yourself with widely used log formats and discover proven methods for data preparation. This course is especially beneficial for roles such as data analysts, IT administrators and log management specialists.

- Format: Instructor-led training
- Duration: 1 day
- Cost: 2 training credits
- Learn More: [LOG 201: Course Syllabus](#)

LOG 202: Analyze Logs, Visualize Data and Answer Business-Critical Questions Using Falcon LogScale

Are you responsible for analyzing data to provide actionable insights for your organization? In this immersive course, you will gain hands-on experience with CrowdStrike Falcon LogScale for analyzing logs, visualizing data and answering business-critical questions. Learn to design compelling widgets and dashboards, optimize dashboard interactions and strategically architect parameterized dashboards using the Falcon LogScale Query Language (LQL). This course is especially beneficial for roles such as data analysts, KIT administrators and log management specialists.

- Format: Instructor-led training
- Duration: 1 day
- Cost: 2 training credits
- Learn More: [LOG 202: Course Syllabus](#)



CROWDSTRIKE
U N I V E R S I T Y

