



**CROWDSTRIKE**  
UNIVERSITY

# TRAINING CATALOG

CROWDSTRIKE SERVICES, INC.

LEARN TO STOP BREACHES

# Table of Contents

Overview and Basic Information	<b>3</b>
Falcon Platform	<b>8</b>
Endpoint Security	<b>13</b>
Next-Gen SIEM	<b>19</b>
Cloud Security	<b>21</b>
Identity Protection	<b>25</b>
Data Protection	<b>27</b>
Threat Intelligence	<b>29</b>
IT and Security Operations	<b>31</b>
Observability and Log Management	<b>34</b>

# 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. At CrowdStrike University (CSU), there is a learning path and certification for you.

- Get started with the Falcon platform
- Gain advanced skills to use on the job
- Prepare to become a CrowdStrike certified professional

## CROWDSTRIKE UNIVERSITY

CrowdStrike University offers all CrowdStrike eLearning, instructor-led training and certification in one place, providing a personalized learning experience for individuals who have an active training subscription.

Access to CrowdStrike University requires a training subscription for each learner. Through CrowdStrike University, you can access:

- **Self-paced fundamentals courses:** Disseminate fundamental Falcon product knowledge and skills through microlearning modules to support anytime access.
- **What's New in Falcon (WNIF):** Learn about CrowdStrike product updates in these short training videos.
- **Quick technical tips (QTTs):** Access quick technical tips for some common problems.
- **Instructor-led training (ILT):** Register for upcoming live course sessions, with the purchase of CrowdStrike training credits, to gain knowledge and skills from CrowdStrike experts and practice in the cloud-based Falcon platform training lab.
- **On-demand instructor-led training:** Register for an on-demand version of our live instructor-led training courses with the purchase of CrowdStrike training credits. This format includes recorded instructor lectures and lab demos, plus 30 days of on-demand CrowdStrike Falcon platform access to complete hands-on lab exercises.
- **CrowdStrike certification:** Register for CrowdStrike certification exams through Pearson VUE, CrowdStrike's test delivery vendor, with the purchase of exam vouchers.

## ACCESSING CROWDSTRIKE UNIVERSITY

To get access to CSU, each named learner must have:

- **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.

Note: CrowdStrike training subscriptions are transferable with documented change of staff — limited to 10% of subscriptions purchased per year.

- **Included content:** All learners with access to CrowdStrike University can view all eLearning fundamentals courses, WNIF videos and QTTS.
- **ILT registration:** To register for an ILT class or an on-demand instructor-led training class, learners must have an active CrowdStrike University account and CrowdStrike training credits.
- **Certification scheduling:** To take a CrowdStrike certification exam, learners are strongly advised to have an active CrowdStrike University account and a CrowdStrike exam voucher. 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](#).

**Need help?** 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](mailto:LMS-Helpdesk@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. For the most up to date course list, view the Content Library in CrowdStrike University.

### Self-Paced eLearning Courses

Designed with interactivity in mind, the self-paced eLearning courses provide fundamental Falcon product knowledge in accessible, micro-learning modules.

### Instructor-Led Training Courses

Take advantage of instructor-led training across multiple days and time zones around the globe, where you can engage with CrowdStrike experts and practice what you learn in class in the cloud-based Falcon lab environment. Check out 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.**

Choose from a range of flexible options, including:

- 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

## Live Onsite Training

You can set up live, onsite instructor-led training as needed for your organization. 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

When scheduling either live online or onsite private instructor-led training classes, there is a 10-student minimum and a 15-student maximum per class/day of instruction.

## Scheduling

Private online and onsite training can be schedule by contacting [training@crowdstrike.com](mailto:training@crowdstrike.com).

## On-Demand Instructor-Led Training Courses

Our on-demand instructor-led training courses offer unparalleled flexibility, allowing you to access and complete courses at your own pace. Once registered, you have access to the lab environment and course materials for 30 days and can:

- View instructor-led videos in smaller increments, allowing you to replay them as needed
- Access online course materials, including job aids and lab guides
- Get hands-on in the Falcon platform lab environment
- Access CrowdStrike expert help through email or the community forum

After the course ends, learners get access to course Student and Reference Guides in a Course Materials add-on course, just like our live learners.

Note that the on-demand courses share many of the same characteristics as our live training courses, including the course title, learning objectives and lab exercises.

## On-Demand Course Registration

To register for an on-demand course, learners must purchase the appropriate number of training credits for the course, and the training credits must be active (not expired) for the 30-day duration of the course. Training credits applied to on-demand instructor-led courses cannot expire during the 30-day on-demand class period. For example, if a learner's training credits expire on April 30, the learner should request approval at least by April 1.

## On-Demand Start Date Considerations

Request enrollment only when you are ready to begin an on-demand course because on-demand courses provide access to the unique Falcon lab environment for 30 days, which begins once the registration request is approved and training credits are processed by the CrowdStrike University team.

## Register for an On-Demand Course

**Search for an on-demand course:** In CSU, enter a search for the desired course and find the corresponding code ending in "a" for asynchronous, on-demand ILT training. You will notice the "a" version of the course should describe the course delivery method as on-demand and have a course length of 30 days.

For example, searching for "FALCON 202" will result in two results. Select falcon 202A for the on-demand course.

Delivery Method	Course Code	Course Title	Credits	Course Length
Live	FALCON 202	Investigating and Querying Event Data with Falcon EDR	2	1 day
On-Demand	FALCON 202A	Investigating and Querying Event Data with Falcon EDR	2	30 days

### Browse for an on-demand course:

- 1 Navigate to the Content Library in CSU.
- 2 From the left-side Filter pane, select **Topics > Course Delivery > On-Demand Instructor-Led Training**.
- 3 Click on the course you'd like to take.

### Enroll in an on-demand course:

- 1 Once on the on-demand course page you'd like to enroll in, scroll down to review the course description and click **Continue this Course**.
- 2 In the Prerequisites/Approval window, click **Request Approval**.

## No Cancellation for On-Demand Training

On-demand courses typically take 7-8 hours to complete. The learner is provided sufficient opportunity to complete the course over 30 days.

Once an on-demand instructor-led training course has been started, the training course cannot be canceled or time extended.

## 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.

# Falcon Platform



# Self-Paced eLearning

## **FALCON 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: 15 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 SOAR Fundamentals**

Falcon Fusion SOAR is a unified and extensible SOAR (security orchestration, automation and response) 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: 22 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

### **FALCON 115: Create a Falcon Fusion SOAR Workflow**

Falcon Fusion SOAR has many possibilities when it comes to building workflows. These workflows can improve the efficiency of an organization's security and IT operations, and allow you to respond more quickly to critical issues! This course provides hands-on practice on creating several sample workflows step-by-step.

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

### **FALCON 175: Falcon Foundry Fundamentals**

Learn about CrowdStrike Falcon® Foundry, a low-code application platform (LCAP) that provides Falcon platform users with the ability to develop IT and security solutions that CrowdStrike does not provide out of the box. This course covers Falcon Foundry's basic architecture (including the UI and CLI); the processes for creating, deploying and releasing apps into your environments; and what kind of apps are able to be created with the tool.

- Format: Self-paced eLearning
- Duration: 30 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

### **FALCON 185: Falcon for IT Fundamentals**

CrowdStrike Falcon® for IT is a new product offering tailored to cater to the workflows and use cases of IT organizations. It empowers users to gain enhanced context from their assets, facilitate patch management and streamline application deployments. With Falcon for IT, users can seamlessly inquire about their assets, review results and execute actions. This course will explain the benefits of Falcon for IT and how to use it effectively.

- Format: Self-paced eLearning
- Duration: 30 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: 20 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

The image features a solid red background. In the center, the words "Endpoint Security" are written in a bold, white, sans-serif font, stacked vertically. The text is positioned to the left of a large, decorative graphic consisting of numerous thin, black, curved lines that sweep across the right side of the frame, creating a sense of motion and depth.

# 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

### **FALCON 151: Incident Workbench Fundamentals**

This course provides learners with a comprehensive overview of the new Incident Workbench available in the Falcon console. The Incident Workbench provides analysts with a single graph view of an incident and provides them with essential tools to identify detection sources, provide meaningful remediation solutions and utilize enrichment capabilities such as Intel and Sandbox.

- Format: Self-paced eLearning
- Duration: 20 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.

- Format: [Live instructor-led training](#) or [On-demand 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.



# **Next-Gen SIEM**

# Self-Paced eLearning

## SIEM 100: Next-Gen SIEM Fundamentals

This course dives into the fascinating world of next-generation security information and event management (SIEM). Whether you are a cybersecurity professional, a system administrator or someone curious about the latest in security technology, this course will equip you with a solid understanding of what SIEM is, what CrowdStrike Falcon® Next-Gen SIEM is, how it has evolved, what it means for the future of security and additional references to learn more.

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

# Instructor-Led Training

## SIEM 210: Onboarding Third-Party Data and Managing Falcon Next-Gen SIEM

In this course, you'll learn how to integrate third-party data sources into the CrowdStrike Falcon platform using the CrowdStrike Parsing Standard and Falcon Data Connectors. Additionally, you'll learn to monitor data ingestion volumes and ensure the health and performance of your connectors, enhancing your organization's security posture and operational efficiency.

- Format Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [SIEM 210: Course Syllabus](#)

## SIEM 211: Incident Response and Investigation in Falcon Next-Gen SIEM

Master CrowdStrike Falcon Next-Gen SIEM with this targeted course for security leads, investigators, hunters, security analysts and security operations specialists. Get hands-on experience in investigating third-party data in Falcon Next-Gen SIEM, correlating events, utilizing CrowdStrike Falcon Fusion SOAR automations leveraging Falcon Next-Gen SIEM capabilities, and monitoring and analyzing third-party data.

- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: [SIEM 211: Course Syllabus](#)

# Cloud Security

The image features a solid red background. In the center-left, the words "Cloud" and "Security" are stacked vertically in a bold, white, sans-serif font. On the right side, there are several thin, black, curved lines that sweep from the top right towards the center. On the bottom left, there are also several thin, black, curved lines that sweep from the bottom left towards the center. These lines create a sense of motion and depth.

# 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: 25 minutes
- Cost: Included with LMS Annual Subscription or Customer Access Pass

## **CLOUD 123: Cloud Security Posture Fundamentals**

In this course, you will learn how CrowdStrike's cloud security posture management (CSPM) and cloud infrastructure entitlement management (CIEM) tools can help you keep your cloud data secure and meet industry cloud security recommendations. Discover how to find recommended remediations so that 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: 40 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 125: Managing Cloud and Container Assets**

Do you know all of the assets that exist in your cloud or hybrid environment? If you don't know what is in your environment, it can be difficult to protect it. In this course, you will learn how to review your cloud, physical server and container asset inventory to determine the health of your cloud environment. Learn tips and tricks for successfully searching through your assets to find and fix potential threats in a hybrid cloud environment.

- Format: Self-paced eLearning
- Duration: 45 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**

The image features a solid red background. In the center-left, the words "Identity" and "Protection" are stacked vertically in a bold, white, sans-serif font. On the right side, there is a decorative graphic consisting of several parallel, black, curved lines that sweep from the top right towards the bottom right. A similar graphic of curved lines is also visible in the bottom left corner.

# 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**

The image features a solid red background. In the center-left, the words "Data" and "Protection" are stacked vertically in a bold, white, sans-serif font. On the right side, there is a decorative graphic consisting of several parallel, curved black lines that sweep from the top right towards the bottom right. A similar graphic of curved black lines is also visible in the bottom left corner.

# 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

The image features a solid red background. In the center, the words "Threat" and "Intelligence" are stacked vertically in a bold, white, sans-serif font. On the right side, there is a decorative graphic consisting of several parallel, curved black lines that sweep from the top right towards the center. A similar graphic of curved black lines is visible in the bottom left corner.

# 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: 60 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

# **IT and Security Operations**

The background is a solid red color. On the right side, there are several curved black lines that sweep from the top right towards the bottom right. On the bottom left side, there are several curved black lines that sweep from the bottom left towards the top left. These lines are parallel to each other and create a sense of motion or a stylized wave pattern.

# 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: Vulnerability Management 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: Asset Management 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 123: Configuration Assessment Fundamentals

Configuration Assessment is a capability within Falcon Exposure Management. It evaluates the configuration of assets in your environment and compares them to Center for Internet Security (CIS) Benchmarks for security hardening and misconfigurations, and it assists with compliance needs. With the help of Configuration Assessment, you can strengthen your environments against common attack techniques, meet security and compliance requirements, and prepare evidence for reporting.

- Format: Self-paced eLearning
- Duration: 30 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

The background is a solid red color. On the right side, there are several black curved lines that sweep from the top right towards the bottom right. On the bottom left side, there are several black curved lines that sweep from the bottom left towards the top left. The text is centered in the middle of the page.

# **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 101 before starting any LOG eLearning courses. This will provide the necessary foundation you need for the Falcon platform and CrowdStrike Query Language.

### FALCON 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: 15 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

# Instructor-Led Training

## **LOG 200: Managing and Administering Falcon LogScale (CrowdStrike Hosted)**

The Managing and Administering Falcon LogScale (CrowdStrike Hosted) 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: 1 day
- Cost: 2 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

