CROWDSTRIKE

CROWDSTRIKE
University

TRAINING CATALOG

CROWDSTRIKE SERVICES, INC.

LEARN TO STOP BREACHES

Table of Contents

Overview and Basic Information	**3**
Falcon Platform	**8**
Endpoint Security	**14**
Next-Gen SIEM	**20**
Cloud Security	**26**
Identity Protection	**31**
Data Protection	**34**
Threat Intelligence	**36**
IT and Security Operations	**38**
Log Management Platform	**41**
SaaS Security	**44**

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 course 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 preparation resources in one place, providing a personalized learning experience for all users with access to Falcon.

Through CrowdStrike University, you can access:

- **Self-paced fundamentals courses:** Gain essential Falcon product knowledge and skills through concise microlearning modules, designed for flexible, anytime access.
- **What's New in Falcon (WNIF):** Learn about CrowdStrike product updates in these short training videos.
- **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 resources:** Enroll in recommended learning plans to help you prepare for certification; assess your certification exam readiness with practice exams; and register for certification exams through Pearson VUE with the purchase of exam vouchers.

ACCESSING CROWDSTRIKE UNIVERSITY

CrowdStrike University Fast Track is a complimentary training program included with your active CrowdStrike Falcon® subscription, offering unlimited access to 100-level eLearning courses. It helps enhance your team's expertise with using the Falcon platform to stay ahead of cyber threats.

Organizations with an active CrowdStrike Falcon subscription and access to the Falcon platform or CrowdStrike Customer Center are eligible for CrowdStrike University.

Accessing CrowdStrike University is simple:

- **From the CrowdStrike Customer Center:** Log in and select CrowdStrike University from the left-hand menu.
- **From the Falcon platform:** Navigate to Support and Resources > Support Portal to access the CrowdStrike Customer Center.
- **For partners:** Contact your CrowdStrike Alliance Manager or email alliances_operations@crowdstrike.com to activate your account.

- **Instructor-led training (ILT) registration:** To register for an ILT class or an on-demand instructor-led training class, learners must have pre-purchased sufficient CrowdStrike training credits.
- **Certification exam registration:** CrowdStrike certification exams are delivered globally at test centers and online by Pearson VUE. Learners are required to have an account with Pearson VUE to register for exams; it is strongly recommended that you have an active CrowdStrike University account and exam voucher. Learners can schedule their exam at pearsonvue.com/crowdstrike.

Need help? Contact your account executive to purchase 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.

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 Course Catalog in CrowdStrike University.

Our courses are designed to guide you through progressive skill development, from foundational knowledge to advanced expertise.

- **100-level courses:** Cover fundamentals and essential skills for beginners or those seeking a solid foundation.
- **200-level courses:** Provide intermediate skills and practical applications to enhance proficiency.
- **300-level courses:** Focus on advanced training, complex topics and specialized techniques for expert-level growth.

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 access to CrowdStrike University.

Choose from a range of flexible options, including:

- 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, a video conferencing platform. 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 maximum of 15 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 scheduled by contacting 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 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

Browse for an on-demand course:

1. Sign in to CrowdStrike University through the CrowdStrike Customer Center.
2. Select the Menu icon in the upper left corner.
3. Select Course Catalog.
4. In the Filter search bar, enter "On-Demand" and select the search icon or hit enter.
5. Select the course you would like to take.

Enroll in an on-demand course:

6. Review the course description and click Enroll.
7. All registration requests are reviewed by our registration team. If your company has purchased CrowdStrike training credits, you will be approved to take the training in 1-2 business days. Once your registration request is confirmed, you will receive an email confirmation with the session details.

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 have time extended.

CROWDSTRIKE FALCON CERTIFICATION PROGRAM

The CrowdStrike Falcon Certification Program (CFCP) validates the knowledge and skills of CrowdStrike users with certification exams aligned to job roles and product knowledge. Exams measure proficiency with use of the Falcon platform and features. Earning a credential highlights your skills and is a recognition of your commitment to keeping pace with rapidly changing technology and professional growth.

Available certifications include:

- CrowdStrike Certified Falcon Administrator (CCFA)
- CrowdStrike Certified Falcon Responder (CCFR)
- CrowdStrike Certified Falcon Hunter (CCFH)
- CrowdStrike Certified SIEM Engineer (CCSE)
- 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 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. Candidates have ninety (90) minutes to complete the exam. At the conclusion of an exam, candidates will receive a score report including a summary of their performance by exam section. Successful candidates will receive a digital badge from Credly to share their certified status on social media.

Falcon Platform

Last Updated: November 12, 2025

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 covers the basics of Falcon's architecture, including endpoint and cloud security, exposure management, next-generation SIEM, data and identity protection, and Counter Adversary Operations.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

FALCON 101: Falcon Platform Essentials

This course offers a guided tour of the Falcon console, showcasing key applications and capabilities that support threat detection, prevention, and response. You'll learn how different features are used by various roles across your security team and gain a foundational understanding of how the Falcon platform helps protect your organization.

- Format: Self-paced eLearning
- Duration: 50 minutes
- Cost: Included with access to CrowdStrike University

FALCON 102: Falcon Platform Onboarding Configuration

The CrowdStrike Falcon platform stops breaches through cloud-delivered technologies, and getting it set up requires a number of important steps. In this course, you will identify which administrative tasks are necessary to get CrowdStrike Falcon up and running in your environment as well as providing the recommended order to complete them.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

FALCON 103: Introduction to Kestrel

This course will provide you a comprehensive introduction to Kestrel, CrowdStrike's new user interface. It will guide you through the essential features and workflows of the Kestrel user interface, empowering you to navigate and utilize the Falcon platform efficiently.

- Format: Self-paced eLearning
- Duration: 40 minutes
- Cost: Included with access to CrowdStrike University

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: 20 minutes
- Cost: Included with access to CrowdStrike University

FALCON 105: Sensor Installation, Configuration and Troubleshooting

Learn how to install, configure, and troubleshoot Falcon sensors. This course presents the sensor pre-installation considerations, installation examples and options, installation configuration, and how to troubleshoot common installation issues.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

FALCON 106: Customizing Dashboards in Falcon

Falcon customizable dashboards help you see preconfigured views of commonly useful detection data. In this brief course, you will learn how to create your own customized dashboards to use privately or share with other users in your organization.

- Format: Self-paced eLearning
- Duration: 15 minutes
- Cost: Included with access to CrowdStrike University

SOAR 100: Falcon Fusion SOAR Fundamentals

CrowdStrike Falcon® Fusion SOAR is a unified and extensible security orchestration, automation, and response (SOAR) framework purpose-built in the CrowdStrike Falcon platform to orchestrate and automate simple and complex workflows. In this course, you will learn how the workflow builder can be used to define how the Falcon platform will respond to certain triggers like incidents, detections, cloud security findings, updates made by users, and more.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

FALCON 141: Charlotte AI Fundamentals

Learn how to use CrowdStrike Charlotte AI™, CrowdStrike's generative, agentic AI assistant, to streamline security operations through natural language prompts. Explore how to analyze threats, automate responses, and apply Charlotte AI in real-world SOC scenarios. By the end of the course, you'll be equipped to integrate Charlotte AI into daily workflows and respond to incidents faster.

- Format: Self-paced eLearning
- Duration: 50 minutes
- Cost: Included with access to CrowdStrike University

FALCON 151: Incident Workbench Fundamentals

This course provides learners with a comprehensive overview of the 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 access to CrowdStrike University

FALCON 175: Falcon Foundry Fundamentals

Learn to build custom applications using CrowdStrike Falcon Foundry to extend your organization's security capabilities. This course provides cybersecurity professionals, application developers, and SOC analysts with essential knowledge to create tailored security solutions. Explore core Falcon Foundry concepts, develop proficiency with the Falcon Foundry CLI and App Builder UI, and explore creating and deploying custom applications with API integrations and workflow templates.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

FALCON 176: Developing Custom Automations with PSFalcon

This course introduces the CrowdStrike API software development kit (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: 1 hour
- Cost: Included with access to CrowdStrike University

FALCON 177: Building API Integrations with FalconPy

Learn to develop custom Python applications using the FalconPy SDK to interact with CrowdStrike Falcon platform APIs programmatically. This self-paced course equips cybersecurity professionals, developers, and analysts with skills for building integrations with the CrowdStrike ecosystem. Learn how you can implement authentication mechanisms, utilize Service Classes and Uber Class approaches, and configure debugging solutions to enable automated threat response and security orchestration workflows.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

FALCON 180: Falcon Forensics Fundamentals

This course offers a thorough understanding of Falcon Forensics, including its data collection, functionality, and deployment on specific hosts for efficient analysis. Learn to customize security solutions using Forensics APIs and navigate dashboards to interpret collected data effectively.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

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 access to CrowdStrike University

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 access to CrowdStrike University

CQL 102: CrowdStrike Query Language Fundamentals 2

This course provides learners with the basic understandings needed to write more efficient queries and effectively troubleshoot problematic queries in the CrowdStrike Query Language. Participants will learn about the CQL execution order, system limits, strategies for writing better queries and best practices.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

Instructor-Led Training

FALCON 200: Falcon Platform for Administrators

This course equips Falcon Administrators with the skills to configure and manage the CrowdStrike Falcon platform for optimal endpoint protection. It covers sensor deployment, policy setup, and host group management, along with using dashboards and reports to assess security coverage. Additionally, participants will learn how to enhance threat detection with indicator of compromise (IOC) management and exclusions.

- Audience: Security administrators and IT operations staff responsible for platform deployment and management
- 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: Exam Guide

Follow the recommended Falcon Administrator courses in CrowdStrike University to prepare for CCFA certification.

Endpoint Security

Last Updated: November 12, 2025

Self-Paced eLearning

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 access to CrowdStrike University

CQL 102: CrowdStrike Query Language Fundamentals 2

This course provides learners with some basic understandings needed in order to write more efficient queries and effectively troubleshoot problematic queries in the CrowdStrike Query Language. Participants will learn about the CQL execution order, system limits, strategies for writing better queries, and best practices.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

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: 20 minutes
- Cost: Included with access to CrowdStrike University

FALCON 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 access to CrowdStrike University

FALCON 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 access to CrowdStrike University

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: 25 minutes
- Cost: Included with access to CrowdStrike University

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: 15 minutes
- Cost: Included with access to CrowdStrike University

FALCON 124: Discover for IoT Fundamentals

Critical infrastructure systems are vulnerable to cyberattacks, requiring security for industrial control systems (ICS) alongside information technology (IT) and operational technology (OT) assets. Falcon Discover for IoT extends security hygiene across these environments. This course covers using the ICS collector to gather IT, OT, and IoT device data, navigating the Discover IoT dashboard, examining asset data, and defining key terms.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

FALCON 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: 30 minutes
- Cost: Included with access to CrowdStrike University

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: 1 hour
- Cost: Included with access to CrowdStrike University

FALCON 150: Incidents Fundamentals

Learn the fundamentals of Endpoint security > 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: 20 minutes
- Cost: Included with access to CrowdStrike University

FALCON 151: Incident Workbench Fundamentals

This course provides learners with a comprehensive overview of the 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 access to CrowdStrike University

FALCON 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: 15 minutes
- Cost: Included with access to CrowdStrike University

Instructor-Led Training

CQL 201: Designing and Optimizing CQL Queries

Learn advanced CrowdStrike Query Language (CQL) techniques to enhance your security investigations and data analysis capabilities. This comprehensive course teaches cybersecurity professionals to construct efficient queries, optimize performance, and create meaningful visualizations across the CrowdStrike Falcon platform and Falcon Next-Gen SIEM. Participants will apply advanced query techniques including aggregation and joins, design parameterized queries for reusable analysis, and develop skills to resolve query performance issues while creating compelling data visualizations for various audiences.

- Audience: Security analysts, threat hunters, and incident responders who query security data
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: CQL 201: Course Syllabus

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.

- Audience: Security analysts and incident responders who investigate and respond to security incidents using Falcon Insight XDR
- Format: Live instructor-led training or On-demand Instructor-led
- 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.

- Audience: Security analysts and investigators who use Falcon Insight XDR for threat detection and incident response
- 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.

- Audience: Falcon Real Time Responders, security analysts, and incident response teams who perform host-level investigations and remediation
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: FALCON 240: Course Syllabus

FALCON 280: Investigating with Falcon Forensics

Enhance your forensic investigation capabilities with CrowdStrike Falcon® Forensics, a comprehensive tool for collecting and analyzing on-disk artifacts during host-based investigations. This specialized course equips incident response analysts and threat hunters with skills to navigate Falcon Forensics dashboards and leverage CrowdStrike Query Language (CQL) syntax. Participants will master key features including Windows hunting leads, Host timeline, and Host info dashboards while conducting thorough investigations through hands-on exercises and a comprehensive capstone project.

- Audience: Incident response analysts and threat hunters expanding capabilities with Falcon Forensics
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: FALCON 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.

- Audience: Threat hunters, cyber defense incident responders, security analysts, SOC analysts, and threat analysts
- 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.

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: Exam Guide

Follow the recommended Falcon Responder courses 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 detections within the Falcon console, including use of pre-built queries and reports and creating custom queries using CrowdStrike Query Language (CQL).

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: Exam Guide

Follow the recommended Falcon Hunter courses in CrowdStrike University to prepare for CCFH certification.

Next-Gen SIEM

Last Updated: November 12, 2025

Self-Paced eLearning

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 access to CrowdStrike University

CQL 102: CrowdStrike Query Language Fundamentals 2

This course provides learners with some basic understandings needed in order to write more efficient queries and effectively troubleshoot problematic queries in the CrowdStrike Query Language. Participants will learn about the CQL execution order, system limits, strategies for writing better queries, and best practices.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

ONUM 100: Falcon Onum Foundations and Overview

This introductory course provides a high-level understanding of Falcon Onum — what it is, why it matters, and how it fits within CrowdStrike's data and security ecosystem. Participants will explore Falcon Onum's core capabilities, its value in streamlining data pipelines, and the foundational architecture that powers it. Ideal for anyone new to Falcon Onum or seeking to understand its strategic role within the Falcon platform portfolio.

- Format: Self-paced eLearning
- Duration: 40 minutes
- Cost: Included with access to CrowdStrike University

ONUM 101: Getting Started with the Falcon Onum Console

In this course, learners will explore the Falcon Onum console and gain hands-on knowledge of its core components and configuration workflows. Through guided demonstrations, you'll learn how to set up listeners and data sinks, perform the main "tenant" administration tasks, apply labels for data traffic organization/categorization, and understand how it is possible to enrich data within the platform. By the end of the course, you'll be able to confidently configure and navigate your Falcon Onum environment.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

ONUM 102: Building and Managing Pipelines

Dive deeper into Falcon Onum's core functionality — designing, building, and optimizing data pipelines end-to-end. In this course, learners will be guided through the full pipeline, from defining inputs (Listeners) and destinations (Data Sinks) to assembling and sequencing Actions using the Actions tab. You'll explore how to apply Transformations, Filters, and the Message Builder formatting action to structure, tailor, and deliver your data flows. Upon completion, participants will be confident building meaningful pipelines in Falcon Onum.

- Format: Self-paced eLearning
- Duration: 1 hour and 30 minutes
- Cost: Included with access to CrowdStrike University

SIEM 100: Next-Gen SIEM Fundamentals

This course dives into the fascinating world of next-generation security information and event management (SIEM). Whether you're brand new to SIEM or looking to build a solid foundation in next-generation tools, this course will equip you with the knowledge to navigate and use CrowdStrike Falcon Next-Gen SIEM.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

SIEM 105: Falcon Next-Gen SIEM Architecture and Core Concepts

This course introduces learners to the architecture, data processing pipeline, and strategic planning considerations behind CrowdStrike Falcon Next-Gen SIEM. Participants will explore core system components including real-time processing, index-free data organization, and complex data formatting.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

SIEM 106: Case Management Fundamentals

This course introduces CrowdStrike's unified Case management system, designed to replace legacy Incidents with a centralized, platform-wide solution for tracking, investigating, and resolving security events. Learners will explore how to manage Cases efficiently, from creation to resolution, using templates, notification groups, and SLAs to ensure accountability and streamline workflows.

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with access to CrowdStrike University

SIEM 107: Creating Correlation Rules with Falcon Next-Gen SIEM

Learn how to create, test, and maintain effective correlation rules in the Falcon platform. This practical, hands-on course guides you through the essential steps of using templates to create correlation rules that help detect potential security threats in your environment. Through interactive exercises and real-world scenarios, you'll learn how to use correlation rule templates to deliver high-quality dections for common use cases.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

SIEM 108: Managing Automation Workflows with Fusion SOAR in Falcon Next-Gen SIEM

Learn to build efficient alert management workflows using Falcon Next-Gen SIEM to reduce alert fatigue and optimize SOC operations. This course guides cybersecurity professionals through configuring the Falcon Fusion SOAR workflow engine to create targeted notification strategies for awareness, operational, and security escalation alerts. Through hands-on configuration exercises, you'll develop practical skills in implementing smart filtering, automating decision-making processes, and aligning alerting with risk levels to improve overall SOC efficiency.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

FALCON 151: Incident Workbench Fundamentals

This course provides learners with a comprehensive overview of the 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 access to CrowdStrike University

Instructor-Led Training

CQL 201: Designing and Optimizing CQL Queries

Learn advanced CrowdStrike Query Language (CQL) techniques to enhance your security investigations and data analysis capabilities. This comprehensive course teaches cybersecurity professionals to construct efficient queries, optimize performance, and create meaningful visualizations across the CrowdStrike Falcon platform and Falcon Next-Gen SIEM. Participants will apply advanced query techniques including aggregation and joins, design parameterized queries for reusable analysis, and develop skills to resolve query performance issues while creating compelling data visualizations for various audiences.

- Audience: Security analysts, threat hunters, and incident responders who query security data
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: CQL 201: Course Syllabus

SIEM 200: Administering and Optimizing Falcon Next-Gen SIEM

Learn essential administration and optimization techniques for CrowdStrike Falcon Next-Gen SIEM to establish secure, efficient enterprise security operations. This comprehensive course equips SIEM administrators, security architects, and infrastructure support specialists with critical skills for managing enterprise-scale deployments. Participants will learn about role-based access controls, implement various data ingestion methods and connectors, and apply fleet management strategies to efficiently manage log collectors and streamline data onboarding processes. Through hands-on exercises, attendees will develop proficiency in system monitoring, parser management, and troubleshooting techniques essential for maintaining optimal SIEM performance.

- Audience: Falcon platform administrators, Falcon Next-Gen SIEM administrators, security architects, infrastructure support specialists, and security engineers
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: SIEM 200: Course Syllabus

SIEM 210: Onboarding and Managing Data Sources in Falcon Next-Gen SIEM

Learn to onboard and manage data sources in CrowdStrike Falcon Next-Gen SIEM to establish reliable data pipelines for security operations. This course equips system administrators, security engineers, and data managers with essential skills for data source integration, connection configuration, and data normalization using CrowdStrike Parsing Standard (CPS). Through hands-on exercises, participants configure data connectors, implement proper parsing techniques, and establish monitoring protocols to ensure optimal data flow. Gain practical experience managing the complete data pipeline lifecycle, from initial connection setup to ongoing maintenance and troubleshooting.

- Audience: Falcon platform administrators, Falon Next-Gen SIEM administrators, data managers, security architects, infrastructure support specialists, and security engineer/data custodians
- 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.

- Audience: Incident responders, global SOC analysts, Falcon Next-Gen SIEM analysts, security leads, and customers who have purchased CrowdStrike Falcon Insight XDR or Falcon Next-Gen SIEM
- Format: Live instructor-led training or On-demand Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: SIEM 211: Course Syllabus

Certification

CrowdStrike Certified SIEM Engineer (CCSE)

The CrowdStrike Certified SIEM Engineer (CCSE) exam is the final step toward the completion of the CCSE certification. This exam evaluates a candidate's knowledge, skills, and abilities to implement and manage CrowdStrike Falcon Next-Gen SIEM to support security operations.

- Exam Questions: 60
- Duration: 90 minutes
- Learn More: Exam Guide

Access the recommended SIEM Engineer courses in CrowdStrike University to prepare for CCSE certification.

Cloud Security

Last Updated: November 12, 2025

Self-Paced eLearning

CLOUD 090: Introduction to Cloud Computing

Introduction to Cloud Computing is a beginner-friendly course designed to help learners understand the fundamental concepts, benefits, and models of cloud computing. Whether you're a student exploring IT for the first time or a professional seeking to broaden your technical knowledge, this course provides a clear and practical overview of how cloud services work and why they are transforming the way businesses operate.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

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: 45 minutes
- Cost: Included with access to CrowdStrike University

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, while also meeting industry cloud security recommendations. Discover how to find recommended remediations so you can address potential threats in your cloud environment such as misconfigurations, exposed cloud assets, and overprivileged cloud accounts.

- Format: Self-paced eLearning
- Duration: 40 minutes
- Cost: Included with access to CrowdStrike University

CLOUD 124: Falcon Cloud Security Registration and Configuration

Learn to establish secure, compliant cloud infrastructure using CrowdStrike Falcon® Cloud Security across multi-cloud environments. This course equips security and cloud professionals with essential skills to register, configure, and operationalize CSPM for AWS, Azure, OCI, and Google Cloud platforms.

- Format: Self-paced eLearning
- Duration: 26 minutes
- Cost: Included with access to CrowdStrike University

CLOUD 125: Managing Cloud and Container Assets

Learn to achieve comprehensive visibility and protection across cloud, physical server, and container assets using CrowdStrike Falcon Cloud Security in hybrid environments. This course equips cloud security professionals with essential skills to identify and manage assets across multi-cloud infrastructures. Participants will develop expertise in leveraging Falcon Cloud Security for monitoring workloads and utilizing attack path visualization tools. Through practical exercises, learners will gain hands-on experience enforcing security policies and implementing remediation strategies.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

CLOUD 170: CrowdStrike Runtime Security Fundamentals

Securing containerized workloads at runtime is vital in dynamic cloud environments. This course teaches you to set up, monitor, and secure containers using Falcon Cloud Security tools like prevention policies, Kubernetes Admission Controller, and the Falcon sensor for Linux. Through hands-on scenarios, you'll learn to identify and prioritize runtime risks and detect and prevent threats such as malware and rogue containers.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

CLOUD 173: Shifting Left with Falcon Cloud Security

Traditional methods of vulnerability management by scanning workloads as they run are not feasible, and leave out DevOps. This course provides tips and best practices on how to use Falcon Cloud Security to "shift left" and find risky containers before they are deployed into production. You will learn to use tools such as image assessment policies, infrastructure as code assessments, and image registries while also learning how to collaborate with DevOps to maintain secure images and code.

- Format: Self-paced eLearning
- Duration: 46 minutes
- Cost: Included with access to CrowdStrike University

CLOUD 180: Application Security Posture Management (ASPM) in Falcon Cloud Security

This course is designed for cloud security specialists and risk managers to learn how to use ASPM to gain visibility into the security, data privacy, and operational risk of applications running in the cloud at scale. Participants will use ASPM to monitor, secure, and respond to vulnerabilities in modern applications across various development environments and understand the role of ASPM in their overall security strategy.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

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.

- Audience: System administrators, security analysts, cloud security architects, and compliance managers
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: CLOUD 223: Course Syllabus

CLOUD 271: Securing a Runtime Environment with Falcon Cloud Security

Your containers aren't just at risk during build or deployment — the real battle happens at runtime. In this training, you will learn how to use Falcon Cloud Security and Containers (FCSC) to gain the visibility and control needed to secure your containers at runtime — where the real action is.

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.

- Audience: Cloud security administrators, cloud security analysts, and cloud risk managers
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- 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
- Learn More: Exam Guide

Access the recommended Cloud Specialist courses in CrowdStrike University to prepare for CCCS certification.

Identity Protection

Last Updated: November 12, 2025

Self-Paced eLearning

IDP 170: Falcon Identity Protection Fundamentals

Learn how to detect and prevent identity-based threats using behavioral analytics that build user profiles to identify suspicious activities across on-premises, cloud, and hybrid environments. In this course, you'll develop essential skills for monitoring authenticated user behavior, analyzing security risks, implementing Zero Trust policies, and configuring multifactor authentication to secure your organization's identities without disrupting legitimate business activities.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

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 access to CrowdStrike University

Instructor-Led Training

IDP 270: Securing Workforce Identities with Falcon Next-Gen Identity Security

Strengthen your organization's defense against credential-based attacks with CrowdStrike Falcon® Next-Gen Identity Security. This comprehensive course teaches security professionals how to effectively implement and leverage Falcon Next-Gen Identity Security's powerful capabilities to protect workforce identities through a Zero Trust approach. Participants will learn to configure advanced identity protection controls, monitor authentication activities, and enhance visibility into your domains and security posture.

- Audience: Identity protection administrators, identity protection policy managers, identity protection domain administrators, and Falcon investigators
- 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
- Learn More: Exam Guide

Follow the recommended Identity Specialist courses in CrowdStrike University to prepare for CCIS certification.

Data Protection

Last Updated: November 12, 2025

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 access to CrowdStrike University

Threat Intelligence

Last Updated: November 12, 2025

Self-Paced eLearning

CTI 130: CrowdStrike Falcon Intelligence Fundamentals

Learn where to find information and intelligence in CrowdStrike Falcon Counter Adversary Operations and how to use it. This course covers various workflows for the use of intelligence, reports, threat actors, tailored intelligence, the new malware and hunting AI agents, and summary recommendations.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

IT and Security Operations

Last Updated: November 12, 2025

Self-Paced eLearning

ITSEC 120: Falcon Exposure Management Fundamentals

CrowdStrike Falcon® Exposure Management is an 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 access to CrowdStrike University

ITSEC 121: Vulnerability Management Fundamentals

Falcon Vulnerability Management (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 access to CrowdStrike University

ITSEC 122: Asset Management Fundamentals

Falcon Asset Management (Discover) is CrowdStrike's IT hygiene module. Falcon Asset Management 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 Asset Management 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 access to CrowdStrike University

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 access to CrowdStrike University

ITSEC 124: Network Scanning Fundamentals

This fundamentals course introduces learners to CrowdStrike's Network scanning capabilities. Participants will learn how to configure, manage, and execute scans across networks to identify asset inventory and vulnerabilities, especially for systems without Falcon sensors.

- Format: Self-paced eLearning
- Duration: 25 minutes
- Cost: Included with access to CrowdStrike University

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 access to CrowdStrike University

ITSEC 128: Falcon External Attack Surface Management Fundamentals

With the external attack surface management (EASM) functionality in Falcon Exposure Management, 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 EASM and how to use EASM effectively.

- Format: Self-paced eLearning
- Duration: 30 minutes
- Cost: Included with access to CrowdStrike University

Log Management Platform

Last Updated: November 12, 2025

Self-Paced eLearning

.

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 access to CrowdStrike University

CQL 102: CrowdStrike Query Language Fundamentals 2

This course provides learners with some basic understandings needed in order to write more efficient queries and effectively troubleshoot problematic queries in the CrowdStrike Query Language. Participants will learn about the CQL execution order, system limits, strategies for writing better queries, and best practices.

- Format: Self-paced eLearning
- Duration: 1 hour
- Cost: Included with access to CrowdStrike University

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 logs 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: 1 hour
- Cost: Included with access to CrowdStrike University

Instructor-Led Training

CQL 201: Designing and Optimizing CQL Queries

Learn advanced CrowdStrike Query Language (CQL) techniques to enhance your security investigations and data analysis capabilities. This comprehensive course teaches cybersecurity professionals to construct efficient queries, optimize performance, and create meaningful visualizations across the CrowdStrike Falcon platform and Falcon Next-Gen SIEM. Participants will apply advanced query techniques including aggregation and joins, design parameterized queries for reusable analysis, and develop skills to resolve query performance issues while creating compelling data visualizations for various audiences.

- Audience: Security analysts, threat hunters, and incident responders who query security data
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: CQL 201: Course Syllabus

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.

- Audience: Log managers/data custodians, and system administrators on a security or IT team
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- 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.

- Audience: IT administrators and log management specialists
- Format: Instructor-led training
- Duration: 1 day | 8 hours
- Cost: 2 training credits
- Learn More: LOG 201: Course Syllabus

SaaS Security

Last Updated: November 12, 2025

Self-Paced eLearning

SAAS 150: Falcon Shield Fundamentals

This course provides a foundational understanding of the SaaS ecosystem and the unique risks it introduces. You'll learn about common SaaS threats, explore real-world vulnerabilities, and discover how CrowdStrike Falcon® Shield delivers visibility, control, and security across SaaS applications. The course also highlights best practices and operational guidance to help you strengthen your organization's SaaS security posture using Falcon Shield.

- Format: Self-paced eLearning
- Duration: 20 minutes
- Cost: Included with access to CrowdStrike University

SAAS 151: Implementing SaaS Security with Falcon Shield

As organizations increasingly rely on SaaS applications to run critical business functions, securing the SaaS ecosystem becomes a top priority. This course is designed to help security professionals build foundational knowledge and strategic skills to implement and manage SaaS security posture management (SSPM) using CrowdStrike Falcon Shield. This course will take you through six key steps for implementing a successful SaaS program at your organization with Falcon Shield.

- Format: Self-paced eLearning
- Duration: 60 minutes
- Cost: Included with access to CrowdStrike University

SAAS 152: Managing SaaS Inventories with Falcon Shield

Learn to implement and operationalize comprehensive SaaS security posture management (SSPM) strategies using CrowdStrike Falcon Shield to protect cloud-delivered applications and data. This course equips cybersecurity professionals with essential skills to gain visibility and control over SaaS environments while mitigating identity-centric threats. Learners will analyze user identities, evaluate application security postures, and implement Zero Trust principles across SaaS platforms, acquiring techniques for detecting shadow IT, responding to data exposure incidents, and enforcing least privilege policies to reduce organizational SaaS attack surfaces.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University

SAAS 153: Monitoring Identities with Falcon Shield

Learn to implement comprehensive identity security programs using CrowdStrike Falcon Shield to monitor, detect, and govern identity threats across SaaS ecosystems. This course equips cybersecurity professionals with essential skills to protect cloud-first organizations from identity-based attacks. Participants will develop expertise in utilizing Falcon Shield's User Inventory and Threat Center for risk assessment, leveraging identity threat detection and response (ITDR) capabilities for threat detection, and implementing governance practices through Permissions Inventory tools. Through hands-on exercises, learners will gain practical experience enforcing least privilege principles and maintaining regulatory compliance across their SaaS environment.

- Format: Self-paced eLearning
- Duration: 45 minutes
- Cost: Included with access to CrowdStrike University


CROWDSTRIKE
University


CROWDSTRIKE