



CrowdStrike University – Overview & Course Catalog

Revised April, 2019

C R O W D S T R I K E S E R V I C E S , I N C .

H E L P I N G Y O U S T O P B R E A C H E S

CrowdStrike University Overview & Course Catalog

CrowdStrike offers professional training and education subscriptions for students from introductory to advanced capabilities. Our education brings out the best in your people, from 24x7 security operations engineers to senior business executives, even those with non-technical responsibilities.

CrowdStrike University Learning Management System (LMS)

CrowdStrike University LMS subscription provides students access to:

- **Self-Paced Courses:** Our self-paced courses have been designed to address the fundamentals of a specific topic. Many of these courses are broken up into “digestible” modules – each being 10-15 minutes in length. The modular nature of these courses allows you to stop and start a course as needed or even jump to a specific module topic.
- **Instructor-Led Courses:** Our instructor-led courses cover a variety of intermediate and advanced topics. These courses are delivered via remote meeting technology providing both lecture and hands-on labs. Some courses are available for on-site training sessions. Each instructor-led course has a pre-fixed training credit cost and students must have access to the CrowdStrike University in order to register to any instructor-led course.
- **How-To Videos / Product Update Video:** In order to give you the latest updates to our products, our Product Update Videos are short / informal training videos that address new features, feature changes and other timely topics. Additionally, our How-To Videos series provides access to quick technical tips for the most common problems that you may face.

CrowdStrike University Subscriptions are sold and assigned on person-by-person named basis. Subscriptions are only transferrable with documented change of staff (limited to 10% of number of licenses purchased per year).

Course Delivery

CrowdStrike’s experience defending the most important organizations, information and networks powers these education offerings. Experienced instructors and responders teach these courses, drawing on the real-world lessons from these incidents.

Some courses are delivered in a self-paced on-line format, which students can consume at a pace and time that is appropriate for their needs. Others are offered with interactive instruction: some of these instructor-led courses can be delivered via remote meeting technology, and some can be delivered at the client’s site.

Courses vary from about 30 minutes for simple how-to topics up to 24 hours for more advanced skills development. Many courses have lab exercises so students can demonstrate their learning; some of those are derived from real incidents.

All courses can be offered remotely or on site. On-site courses are conducted eight hours at a time to maximize students' productivity and interaction with the instructors.

On-site courses require at least two days of training (any courses) and will include a 4 Training Credit surcharge for domestic travel and 6 Training Credit surcharge for international travel (per week).

Both remote and on-site courses have a 6 student minimum and a 15 student maximum per class / day of instruction.

CrowdStrike University Courses

The following self-paced and instructor-led courses are available in CrowdStrike University. Because of the dynamic nature of the product, courses can be added and removed from the catalog as we adapt the courses to address the latest product feature offerings. For the latest course list, please log into CrowdStrike University and go to the online Course Catalog.

All instructor-led courses require each participant to have a subscription to CrowdStrike University.

FHT 100 – Falcon Platform Architecture Overview

Course Number:	FHT 100
Course Length:	30 minutes
Course Cost:	Included with CrowdStrike University subscription
Course Delivery:	Self-paced online
Course Description:	This course describes the various components of the Falcon Platform and how they defend against a typical attack scenario. The course also provides additional details about Falcon Prevent, Falcon Insight, Falcon Intelligence and Falcon Overwatch.

FHT 101 – Falcon Platform Technical Fundamentals

Course Number: FHT 101
Course Length: 4 hours
Course Cost: Included with CrowdStrike University subscription
Course Delivery: Self-paced online
Course Description: This course lays the technical foundation to understand installation, configuration and management of the Falcon Platform. It includes a complete GUI walkthrough.

FHT 105 – Sensor Installation, Configuration and Troubleshooting

Course Number: FHT 105
Course Length: 45 minutes
Course Cost: Included with CrowdStrike University subscription
Course Delivery: Self-paced online
Course Description: This course provides sensor pre-installation considerations, installation examples and options, installation instructions and troubleshooting tips for common installation issues.

FHT 120 – Investigation Fundamentals

Course Number: FHT 120
Course Length: 15 minutes
Course Cost: Included with CrowdStrike University subscription
Course Delivery: Self-paced online
Course Description: The [Investigation Fundamentals](#) course explains what kind of data the Falcon Platform captures, how to access this data through the Falcon Platform interface, and which Falcon Platform apps should be used for different investigation types.

FHT 130 – Falcon Intelligence Fundamentals

Course Number:	FHT 130
Course Length:	30 minutes
Course Cost:	Included with CrowdStrike University subscription
Course Delivery:	Self-paced online
Course Description:	This self-paced course provides students with the fundamentals necessary to make use of the Falcon Intelligence application. It provides an overview of the subscription, with modules about intelligence, reports, threat actors, tailored intelligence, the API and integration points, submitting RFIs and malware for analysis, and summary recommendations.

FHT 200 – Falcon Platform for Administrators

Course Number:	FHT 200
Course Length:	1 day
Course Cost:	2 Training Credits
Course Delivery:	Virtual instructor-led / on-site instructor-led
Course Description:	This course instructs new and beginning users on the technical fundamentals of the Falcon Platform. The course is appropriate for those who use the Falcon Platform on a day-to-day basis, and focuses on the installation, configuration and day-to-day management of the product. This course includes a complete GUI walkthrough.

NOTE: There is a self-paced version of this course available in CrowdStrike University. The instructor-led version of the course is targeted toward students who wish to have a live instructor for the fundamental material.

FHT 201 – Intermediate Falcon Platform for Responders

Course Number: FHT 201
Course Length: 1 day
Course Cost: 2 Training Credits
Course Delivery: Virtual instructor-led / on-site instructor-led
Course Description: This course instructs intermediate responders in the best use of the Falcon Platform for incident triage. The course is appropriate for those who use the Falcon Platform on a day to day basis, focused on triaging and responding to alerts. It includes practical labs for students to develop hands-on skills.

FHT 202 – Intermediate Falcon Platform for Hunters

Course Number: FHT 202
Course Length: 1 day
Course Cost: 2 training credits
Course Delivery: Virtual instructor-led / on-site instructor-led
Course Description: This course instructs intermediate responders in the best use of the Falcon Platform for incident detection using proactive “hunting” investigation. The course is appropriate for those who use the Falcon Platform to find evidence of incidents that did not raise alerts by other means. It includes practical labs for students to develop hands-on skills.

CST 330 – Creating Intelligence with Falcon

Course Number: CST 330

Course Length: 2 days

Course Cost: 4 training credits

Course Delivery: Virtual instructor-led / on-site instructor-led

Course Description: This course introduces the doctrinal concepts of gathering and analyzing information to create intelligence products – it includes Cyber Threat Intelligence methodologies, but is more broadly focused on general intelligence doctrine. This intelligence course is appropriate for techies and non-techies alike who have little or no experience in intelligence functions and production; it is intended for managers, report writers, intelligence consumers, and analysts of all types – there are no prerequisites. It includes practical labs for students to develop hands-on skills.

CST 346 – Structured Analytic Techniques for Cyber Analysts

Course Number: CST 346

Course Length: 1 day

Course Cost: 2 training credits

Course Delivery: Virtual instructor-led / on-site instructor-led

Course Description: Structured Analytic Techniques are scientifically-derived tools analysts can use to abstract their biases out of their own analysis and can also be used to gain insight into the meaning and value of large sets of information. Through the use of these techniques, an analyst is able to provide better accuracy, relevancy, and substance to their intelligence reporting. This course introduces the five core categories of structured analysis and incorporates hands-on exercises of dozens of the individual structured analytic tools. There are no prerequisites.

CST 348 – Operationalizing Falcon Intelligence

Course Number: CST 348

Course Length: 1 day

Course Cost: 2 training credits

Course Delivery: Virtual instructor-led / On-site instructor-led

Course Description: Moving from actionable intelligence to operationally-ready data is an important skillset for cyber analysts. This course covers the pivot from Falcon Intelligence products and IOCs to rule creation and use cases. Various Falcon Intelligence reports and feeds are covered in detail, notably the delimited data structures of feeds and specific procedures commonly needed for security stack implementation. Snort and Yara are covered extensively in this course. This is a hands-on course intended for incident responders and security stack engineers and managers. There are no prerequisites, but previous experience with security tools (Snort, Yara, etc) and networking knowledge is advised.

CST 350 – Deriving Intelligence from Falcon Sandbox

Course Number:	CST 350
Course Length:	1/2 day (4 hours)
Course Cost:	1 training credit
Course Delivery:	Virtual instructor-led / on-site instructor-led
Course Description:	Falcon Sandbox is the most advanced and powerful malware sandbox available. This course enables analysts to utilize Falcon Sandbox's many features and covers the pivot from malware analysis to actionable intelligence. Students will learn how to retrieve Indicators of Compromise (IOC) from file, network, memory, and process activity related to the automated threat analysis available with the sandbox and understand the nature and complexity of the threat by matching indicators to current intelligence. Through this training, security teams will be empowered to gain unprecedented visibility into real-world threats and enable the teams to make faster and better decisions. This course includes numerous hands-on exercises to supplement the training. This hands-on course is intended for incident responders, reverse engineers, and analysts of all types – there are no prerequisites.

CST 351 – Open Source Intelligence Techniques with Falcon

Course Number: CST 351

Course Length: 1 day

Course Cost: 2 training credits

Course Delivery: Virtual instructor-led / On-site instructor-led

Course Description: The Falcon Intelligence application contains an enormous number of artifacts and indicators to properly attribute attacks; however, you can still supplement Falcon Intelligence reporting with your own open source information to provide your organization with holistic and customized intelligence reports. This course introduces the concepts and methodologies needed to successfully extract indicators and artifacts from the CrowdStrike Falcon application and conduct further Open Source Intelligence (OSINT) gathering as part of a larger intelligence reporting effort. It offers hands-on training that covers basic concepts of secure online access and helps you protect your collection efforts. Numerous tools and techniques are introduced to enhance your reporting with openly accessible information from the Internet. This hands-on course is intended for incident responders, reverse engineers, and analysts of all types – there are no prerequisites.