+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on July 15, 2026

Sign Up

CrowdStrike Falcon Training

2 days (14 hours)

Overview

CrowdStrike Falcon is a cloud-native security platform designed to strengthen endpoint protection, accelerate threat detection, and simplify threat response. With its lightweight agent, NGAV capabilities, and unified approach to security, it helps teams effectively stop modern attacks.

Our CrowdStrike Falcon training will take you beyond the basics to master the essential operational uses of a modern security console.

You'll learn how to develop a prevention strategy, understand how policies work, leverage telemetry, and interpret alerts to better assess incidents.

You'll also learn how to manage detections, refine protection rules, handle remediation, and establish consistent monitoring in a production environment.

By the end of the training, you will be able to implement a more robust deployment of CrowdStrike Falcon, reduce operational noise, and strengthen the security posture of your environment.

Finally, this training covers best practices for configuration, monitoring, and administration to ensure the reliable day-to-day use of the platform and support SOC and security administration teams.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the architecture and positioning of CrowdStrike Falcon.
- Configure the main endpoint prevention and protection mechanisms.
- Analyze alerts and use telemetry to assess threats.
- Manage policies, exceptions, and remediation actions.
- Establish an operational framework tailored to a SOC or security administration environment.

Target Audience

- SOC Analyst
- Security Administrator
- Cybersecurity Engineer
- Information Systems Security Manager
- Security Support Technician

Prerequisites

- Basic knowledge of cybersecurity and workstation protection.
- Understanding of Windows principles and system administration.
- Basic knowledge of malware, logs, and incident analysis.
- Previous experience with a security console or EDR is a plus.

Technical Prerequisites

- A recent computer with an up-to-date browser and sufficient resources for demonstrations.
- A stable Wi-Fi or Ethernet internet connection to access remote environments.
- A work environment that allows the use of a secure web console and monitoring tools.
- A microphone and headset are recommended for remote sessions and collaborative workshops.

CrowdStrike Falcon Training Program

[Day 1 - Morning]

Platform Fundamentals

- Understand the role of CrowdStrike Falcon in an endpoint protection strategy.
- Identify key components, including the sensor, the console, and cloud-native logic.
- Distinguish between prevention, detection, and response in an operational workflow.
- Explore the major families of modules and their contribution to security.
- Understand the logic behind the centralization of events and alerts.
- Hands-on workshop: guided introduction to the interface, locating navigation areas, and reading an initial dashboard.

[Day 1 - Afternoon]

Deployment and Initial Protection

- Prepare to deploy the sensor on various workstations.
- Understand the principles of prevention policies and group targeting.
- Analyze configuration options related to real-time protection.
- Manage exclusions, exceptions, and business impacts.
- Monitor the installation status and verify telemetry reporting.
- Hands-on workshop: configuring a basic policy and validating its implementation on a set of test machines.

[Day 2 - Morning]

Detection and Investigation

- Review a detection and understand its key indicators.
- Interpret context, process, and execution history information.
- Link events to an attack chain logic.
- Assess the severity level and prioritize actions.
- Use relevant information to document an incident.
- Hands-on workshop: Analyze real or simulated alerts, then draft an initial operational assessment.

[Day 2 - Afternoon]

Operational Response and Advanced Operations

- Implement remediation actions appropriate to the context.
- Manage the lifecycle of an alert, from opening to closure.
- Apply best practices for monitoring, prioritization, and traceability.
- Structure daily operations to minimize noise and improve efficiency.
- Identify key areas for long-term administration and oversight.
- Hands-on workshop: comprehensive incident handling, from classification through closure and reporting.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific business knowledge or modern methods.

Assessment at the Start of Training

The assessment conducted upon enrollment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their personal expectations and objectives

regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical instruction from the trainer—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.