AMBIENT-IT

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

Updated on 10/09/2026

Sign Up

DFIR-IRIS Training: Collaborative Platform

2 days (14 hours)

Overview

DFIR-IRIS is an open-source collaborative platform dedicated to incident response and digital investigations. It enables SOC, CSIRT, and DFIR teams to centralize incident information, organize evidence and indicators of compromise, and coordinate the various stages of an investigation.

Our DFIR-IRIS training will help you master the platform so you can structure and centralize your cybersecurity investigations, from the initial assessment of an incident through to its closure.

You will learn how to create and organize investigation files, manage analysts' tasks and responsibilities, document events, and centralize the evidence and indicators of compromise (IOCs) needed for analysis.

The training will also enable you to build timelines, enrich the collected information with threat intelligence sources, and leverage integration capabilities with the SOC ecosystem to accelerate investigations.

Finally, you'll discover how to automate certain operations using the DFIR-IRIS API, standardize incident handling procedures, and generate reports that provide an actionable record of investigations and remediation actions.

Upon completion of this training, you will be able to centralize, conduct, and document a cybersecurity investigation using DFIR-IRIS, while improving collaboration and traceability within your incident response teams.

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

Objectives

- Get up to speed with and administer the main features of DFIR-IRIS
- Create and organize incident and investigation files
- Centralize evidence, IOCs, events, and timelines for an investigation
- Organize collaborative work among SOC, CSIRT, and DFIR analysts
- Enhance investigations with threat intelligence sources
- Integrate and automate DFIR-IRIS within a SOC environment
- Document response actions and generate investigation reports

Target Audience

- SOC analysts
- DFIR analysts and consultants
- Forensic analysts
- CSIRT and CERT team members
- Cybersecurity engineers
- Incident Response Managers

Prerequisites

- Knowledge of cybersecurity fundamentals
- Understanding of the main steps in incident response
- Basic knowledge of logs, alerts, and indicators of compromise (IOCs)
- Some experience in a SOC, incident investigation, or operational security is recommended

Technical Prerequisites

- A computer equipped with a recent web browser
- A stable Internet connection
- Access to a DFIR-IRIS lab environment provided or set up for the training

Our DFIR-IRIS Training Program: Collaborative Management of Cybersecurity Incidents

[Day 1 - Morning]

Getting Started with DFIR-IRIS and Organizing the Incident Response

- Discover DFIR-IRIS and its role within a SOC, CSIRT, and DFIR environment
- Understand the platform’s architecture and the key components of an investigation
- Get familiar with the interface, folders, users, groups, and access rights
- Create and structure an investigation case based on a security incident
- Organize the tasks, responsibilities, and information needed for collaborative work

- Understand the principles of traceability and investigation data management
- Hands-on workshop: Create an incident file, organize the investigation team, and structure the initial response actions.

[Day 1 – Afternoon]

Centralize evidence, IOCs, and investigative information

- Collect and organize evidence related to an incident
- Recording and classifying indicators of compromise (IOCs): IP addresses, domains, URLs, files, and hashes
- Document events and build an investigation timeline
- Link technical findings to events and information in the case file
- Use notes, tasks, and comments to facilitate collaboration among analysts
- Structure data to ensure the investigation remains clear, traceable, and actionable
- Hands-on workshop: enrich an incident using IOCs, evidence, and events, then reconstruct the initial stages of a compromise.

[Day 2 - Morning]

Conducting and enriching an investigation with DFIR-IRIS

- Develop a collaborative investigation methodology from initial assessment through remediation
- Leverage information from the case file to identify affected systems, users, and assets
- Enrich indicators using Threat Intelligence sources and tools
- Understand integration possibilities with MISP and external enrichment services
- Organize the information needed to analyze the attack chain
- Track containment, eradication, and remediation actions in the case file
- Hands-on workshop: Conduct an investigation based on an alert, enrich the IOCs, and determine the scope of the compromise.

[Day 2 - Afternoon]

Integrate, automate, and report on investigations

- Understand the possibilities for integrating DFIR-IRIS with SOC, SIEM, EDR, and Threat Intelligence tools
- Leverage the API and automation mechanisms to enrich cases and reduce repetitive tasks
- Standardize the procedures, templates, and information needed to handle incidents
- Create reports that document technical details and actions taken

- Close an incident while preserving the evidence, decisions, and lessons learned necessary for post-incident analysis
- Apply best practices for governance, security, and access control to the platform
- Hands-on workshop: Handling a complete incident, from its opening to its documentation, remediation, and the production of the final report.

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 industry knowledge or modern methodologies.

Assessment at the Start of Training

The pre-training assessment 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 technologies, as well as their expectations and personal goals for 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 Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—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.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg