Updated 06/13/2025

Sign up

Digital Forensics & Incident Response training

4 days (28 hours)

PRESENTATION

Our DFIR training course will enable you to master the essential techniques for effectively managing complex IT incidents and carrying out in-depth forensic analyses. This course covers in detail the advanced methodologies and tools adapted to modern and varied environments such as Windows systems, network infrastructures and SIEM platforms.

In this course, specially designed for advanced security analysts, experienced system and network administrators, and IT security managers and consultants responsible for investigating, responding to and preventing complex incidents.

Through detailed lectures and a series of realistic hands-on workshops, you'll develop direct operational expertise in advanced artifact analysis, network investigation, proactive threat hunting and crisis management. You'll also learn how to integrate these skills into a structured operational framework and produce professional incident reports.

As with all our training courses, it is constantly updated to reflect the latest developments in DFIR.

Objectives

- Explain advanced concepts and DFIR methodologies in detail
- Efficiently structure an advanced DFIR team and manage complex incidents
- Master the use and integration of advanced DFIR tools
- Identify and analyze advanced system and network artifacts in depth
- Implement advanced memory and log analysis techniques
- Automate incident investigation and response processes
- Deploy advanced proactive threat hunting methodologies
- Manage crises effectively and coordinate multidisciplinary teams
- Write detailed and professional incident reports

- Implement proactive incident prevention and response strategies

Target audience

- iT professionals
- System administrators
- Network administrators
- DevOps engineers
- Security Analysts

Prerequisites

- Prior knowledge of fundamental cybersecurity concepts
- Practical experience in the use of basic forensic tools
- Familiarity with Windows operating systems and TCP/IP networks
- Basic scripting skills (Python, PowerShell or Bash)

DFIR training program

Day 1: Advanced introduction to DFIR

Advanced concepts and methodologies

- Essential reminders of the fundamental concepts of DFIR
- Structuring and roles within an advanced DFIR team
- Advanced methods for managing complex incidents
- Prioritization and resource management techniques
- Practical workshop: Setting up and configuring an advanced DFIR environment

Advanced tools and case studies

- Overview and selection of state-of-the-art DFIR tools
- Integration of tools and automation in DFIR workflows
- In-depth study of complex real-life incidents
- Practical workshop: Simulation and analysis of a complex real-life incident
- Best practices in operational safety and prevention

Day 2: Advanced forensic analysis of Windows systems Artifacts

and advanced memory

- Advanced identification and extraction of Windows artifacts

- Extensive registry and event log analysis
- Practical workshop: In-depth analysis of RAM memory
- Using the Volatility and Rekall frameworks
- Advanced malicious activity detection techniques

Advanced log analysis techniques

- Advanced use of Sysmon and Event Tracing
- Detection of suspicious activity and targeted attacks
- Practical workshop: Extracting and analyzing advanced logs
- Investigation of attack techniques (lateral movement, persistence, credential dumping)
- Advanced analysis automation methods

Advanced frameworks and scripting

- In-depth presentation of KAPE
- Scripting and automation to speed up investigations
- Practical workshop: Writing artifact collection scripts
- Optimization of analysis workflows
- Integrity validation and forensic evidence techniques

Day 3: Advanced network analysis and threat hunting

In-depth network traffic capture and analysis

- Advanced PCAP capture analysis techniques
- Advanced use of Zeek and Suricata
- Practical workshop: In-depth identification of network threats
- Detecting malicious activity through behavioral analysis
- Identification and analysis of network anomalies

Proactive threat hunting and automation

- Advanced Threat Hunting methodologies
- Advanced automation and scripting in Threat Hunting
- Practical workshop: Proactive real-time threat hunting
- Advanced use of SIEM platforms
- Technology watch and threat intelligence strategies

Proactive response and prevention tools

- Advanced proactive incident response techniques
- Proactive integration of DFIR into safety policies
- Practical workshop: Implementing an automated proactive response
- Proactive prevention and continuous improvement

- Best practices for integrating DFIR into IT operations

Day 4: Advanced incident management and reporting Coordination and crisis management

- Advanced crisis management techniques
- Coordination of multidisciplinary teams
- Practical workshop: Simulating crisis management in real time
- Effective communication and stakeholder management
- Damage control and restoration techniques

Documentation and reverse engineering

- Advanced DFIR report writing techniques
- Practical workshop: Creating a detailed incident report
- Fast malware reverse engineering techniques
- Optimizing post-incident processes
- Integration of feedback to improve DFIR processes

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.