Publication date : 01/10/2024

Course : Forensic analysis and security incident response

Practical course - 4d - 28h00 - Ref. AFR
Price : 2480 € E.T.

4,2 / 5

This advanced Forensic course will show you the techniques you need to carry out an analysis following the occurrence of IT security incidents. Through numerous simulations, you will learn how to collect, analyze and above all preserve evidence, and thus improve IS security.

Teaching objectives

At the end of the training, the participant will be able to:

- Master the right reflexes in the event of machine intrusion
- Collect and preserve the integrity of electronic evidence
- Analyze intrusion a posteriori
- Improving security after an intrusion

Intended audience

Systems and network engineers/administrators, security managers.

Prerequisites

Good knowledge of IT security and networks/systems.

Practical details

Hands-on work

Investigation of traces of all types, mass memory, collection, analysis, improvement of overall security (implementation of countermeasures).

Course schedule

1 Forensic analysis of systems

- Computer forensics. Types of computer crime.
- Role of the computer surveyor.

PARTICIPANTS

Systems and network engineers/administrators, security managers.

PREREQUISITES

Good knowledge of IT security and networks/systems.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Modern cybercrime

- Types of crime.
- Security incident management framework, CERT.
- Analyze and understand network attacks.
- Network intrusion detection.
- Protection tools, French legislation.

Hands-on work

Analyze network logs of a Volumetric DDoS, ARP. SNORT implementation.

3 Information gathering

- Heterogeneous sources. What is a safety event?
- Security Event Information Management (SIEM), events collected from the IS.
- Equipment system logs (firewalls, routers, servers, databases).

Hands-on work

Address geolocation. Web user history analysis (cookie, POST data). Analyze SQL injection Web logs and implement countermeasures.

4 Log analysis

- Visualize, sort, search in tracks.
- Splunk to understand attacks.

Hands-on work

Install and configure Splunk. Analyze Web logs from a Brute-Force on Form, implement countermeasures.

5 Digital proof

- Definition, role, types and filing rules.
- Evaluate and secure the electronic elements of a crime scene.
- Collect and preserve the integrity of electronic evidence.

Hands-on work

Duplicate data bit by bit, check integrity. Recover deleted and/or hidden files. Analyze digital data.

6 Forensic analysis of a Windows operating system

- Acquisition, analysis and response.
- Understanding start-up processes.
- Collect volatile and non-volatile data.
- How the password system and Windows registry work.
- Analysis of data contained in RAM and Windows files.
- Cache analysis, cookie and browsing history, event history.

Hands-on work

User injection. Break password. Collect, analyze RAM data. Reference and hash all files. Explore browser and registry data.

Dates and locations

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

REMOTE CLASS
2026 : 2 June, 15 Sep., 17 Nov.

PARIS LA DÉFENSE
2026 : 2 June, 15 Sep., 17 Nov.