Cyberdefense

Training Catalogue 2025

Knowledge is power

IR 2.01 | Log Management

Overview

This one-day course covers the fundamentals of event logging on Windows and Linux, the different types of log, and the management and analysis of these logs. It is an ideal complement to the IR1.01 course and aims at examining what needs to be logged and how, so that you can improve your ability to respond to security incidents.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins
- CISO

Skills you'll learn

N/A

Level 2

1 day

French or English

Course Modules

- **Log fundamentals**
  - The good and the bad logs
  - Benefits from the cyber-security point of view
- **Log types**
  - Pros and cons of the various types of logs
- **Log management**
  - Policy definition
  - Compliance requirements
  - Aspects to consider for a strong audit policy
  - Best practices
  - Infrastructure
  - Challenges and common mistakes
  - Logs centralization on Windows and Unix
- **Lab 1 - Data sources identification**
- **Logs analysis**
  - Handling Windows logs
  - Handling Linux logs
  - Rotation and permissions
- **Log management tools**
- **Lab 2 - Logs manipulation on Windows and Linux**