Training Catalogue 2025
Knowledge is power

IR 3.03 | Incident Response (Level 3)

Overview

This intensive hands-on one-day course complements the IR3.01 and IR3.02 courses by covering the fundamentals of mal- ware analysis on Windows. It aims to provide you with the methods and tools you need to carry out basic analyses, using both static and dynamic approaches. You will learn how to quickly assess the threat level of executable files and other Office documents.

Who should attend

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

Skills you'll learn

- **IR 3.02**
- **Level 3**
- **1 day**
- **French or English**

Course Modules

- **Introduction**
  - Objectives
  - Quick reminder of the IR3.02 takeaways
- **Malware Analysis fundamentals**
  - Purpose of malware analysis in the incident response phases
  - Various approaches to malware analysis
  - The main types of malwares
  - Anatomy of sophisticated attacks
- **Basic Static Analysis**
  - Signature-based scan, hashes and IOCs
  - PE analysis
  - Linked libraries and functions
  - Packed and obfuscated malware
  - Office documents
- **Basic Dynamic Analysis**
  - Advantages of controlled environments
  - Sandbox limitations
  - The DIY approach
- **Lab**
  - Understanding the types of malwares and the analysis techniques
  - Playing with a PE through Basic Static Analysis
  - Office document analysis
- **Small game to remember the most important points of the day with fun**

For more information check
www.orangecyberdefense.com/ch

Orange Cyberdefense Switzerland
Rue du Sablon 4, 1110 Morges

training@ch.orangecyberdefense.com
+41 21 802 64 01