Malware : Reverse engineering

Filière : **DevOps & Infrastructure** Sous-filière : **Cyber Sécurité**

RÉFÉRENCE	DURÉE	PRIX UNITAIRE HT
ISMS-MAL	**3 JOURS (21H)**	**1 790 €**

Description

In this course, we address the issue of malware, a major societal concern. IT infrastructures now require security specialists to prevent attacks and analyze the damage caused by malware.
The lesson plan is in three parts :

- What is a malware: taxonomies and different types and capabilities of malware. Analysis of classic schemes of compromises and adjacent infrastructures.
- Malware analysis; Review of the basics needed for Windows process and assembly language operation. Triages techniques, dynamic and static analysis. Use of debugger, decompilers and disassembler. Using flow control graphs. Use of forensic detection tools.
- Technique used by malware; Obfuscations of code, function call and flow. Encryption, polymorphisms and variations, Stealth.

Public cible

- System administrators
- System architects and IT administrators
- Systems engineers

Programme de la formation

What is a malware

- Taxonomies and different types and capabilities of malware
- Analysis of classic schemes of compromises and adjacent infrastructures

Malware analysis

- Review of the basics needed for Windows process and assembly language operation
- Triages techniques, dynamic and static analysis
- Use of debugger, decompilers and disassembler
- Using flow control graphs
- Use of forensic detection tools

Technique used by malware

- Obfuscations of code, function call and flow
- Encryption, polymorphisms and variations, Stealth

Qualité

Cette formation est accessible aux personnes en situation de handicap, nous contacter en cas de besoin d'informations complémentaires.

Programme mis à jour le **6 novembre 2023**