Office Document Analysis

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

RÉFÉRENCE	DURÉE	PRIX UNITAIRE HT
ISMS-OFFICE	**2 JOURS (14H)**	**1 450 €**

Description

We propose a two-day training named «Office documents analysis».
It will enable you to understand how the malwares are using office documents as initial infection stage.

It will help your Incident response team to determine by itself if an office document is malicious.
At the end of the training, you will be able to extract the payload and determine the IOC of a sample.

The training is 50% lectures and 50% lab.

The course will start by a refresh on the current threat landscape. The student will learn how to setup his own office analysis lab and will learn and practise the identification, analyse on various malicious office documents.

The student will learn how obfuscation is in place and how to isolate a shellcode or an malicious payload.

After this formation, the student will be able to qualify the maliciousness of a given office document by his own.

Public cible

- Developers
- System administrators
- Systems engineers

Pré-requis

Knowledge of Linux, Python and scripting

Programme de la formation

The following courses syllabus will be learned :

- Treat landscape
- Setup forensic Lab and Tools
- Why opening theses files & document identification
- Understand how macro deliver payload
- Extraction of Macro
- Macro Goal
- Obfuscation

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**