Build your CSIRT

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

RÉFÉRENCE	DURÉE	PRIX UNITAIRE HT
ISMS-CSIRT4	**4 JOURS (28H)**	**2 600 €**

Description

We propose a 4-day training named «Build your CSIRT». It will enable to understand the needs and the global scope of what is a Computer Security Incident and Response Team (CSIRT). What are the roles in both prevention and incident responses and what will be the required skills and the conduct to have in case of various incidents. It will also allow the to understand the actual threat landscape and allows his team to learn how to perform the triage in order to be able to detect and isolate a rogue malicious code.

Upon this training, you will be capable to understand how to setup your own Computer Security Incident and Response Team and put in place a coherent detection and incident response capacity.

The student will have 4-day training, which should enable him to understand the required skills, processes and needs in order to build his own CSIRT in order to create his own CSIRT Team. Labs session will be done in order to learn how to do basic memory and office document triage.

Public cible

- Administrateurs
- Consultants
- Consultants informatiques
- Développeurs
- Professionnels de l'IT

Pré-requis

The clients should have the basics skills in UNIX commands lines in order to be able to perform the lab activities.

Programme de la formation

Lectures :

Threat Landscape

- Intrusions
    - Motivations
    - Tactics
    - Windows Insecurity & Side steeping
    - APT Groups
- DDOS
    - Detailed attacks tactics
- President fraud & Phishing

Malware Threat Landscape (lecture)

- History: from Virus to Malware, history of evolution towards monetization.
- Taxonomy
- Discovery of different types and capabilities of malware.
- Identification and detection issues.
- Overview of the infrastructures used.
    - Network infrastructures (botnets)
    - DGA.
    - Fastflux networks.
    - Classic schemes of compromise.
- Compromise paths
- Remarkable malware: Overview of current malware families.

Reactions Preparation (detection, reaction, lessons learn and start again)

- Logs preparation
- Time setup
- Security preparation
- What is needed, How to be ready to mitigate (Ids, Honey, RPZ Dns)
- Communications setup
- Why, How, External communication, Public communication

Threat Intelligence

- Goal and Limitations

- Osint Data sources
- Att&ck and Kill Chain framework
- Available tools

Malware analysis essentials

- Objectives of the analysis of a malware.
- Prerequisites for analysis
    - Windows internal operation & user lands process.
    - Introductions to the assembler x86 / 64.
- Identification and detection techniques.
    - Artifacts, Yara, Threat Intelligence
    - Hunting principles
    - Static Analysis vs Dynamic Analysis & Sandboxing.
    - Pros and cons; Decompilers & disassemblers.
    - Obfuscation

The work of a CSIRT Team

- Evidences collection 101
    - How to take evidences (Art of memory and Disk dump)
    - Sandbox (usage, benefits and restrictions)
    - Basic tooling (Volatility, Sysinternals, Detection tools)
- Containment and reactions
    - Appropriate actions to appropriate threats.
    - How to face External Threat
    - How to face Internal threat
- Organisation of a CSIRT team
    - Tools Needed and organisation
    - The SIM3 approach
    - Teams and Organisations

Workshops

- Practical study of a dropper via document office.
    - Office files and script droppers
    - How office documents are used

  - VBA Document analyse
  - VBA Obfuscations
  - Tools for un-obfuscation

- Identification and sorting of a malware from a memory image.
  - Detect and find user land threats
  - Getting started with Volatility, Yara, and Threat intelligence.
  - Static analysis of malware.

- Deployment of a threat Intelligence data bus
  - Hand's on IntelMQ

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**