

## Appropriate Reactions and Answers to External and Internal Threats

Pour comprendre les menaces cybernétiques actuelles, savoir comment se préparer et apprendre à réagir adéquatement !

### Détails

- **Code** : ARAEIT
- **Durée** : 2 jours ( 14 heures )

#### Public

- Administrateurs systèmes
- Administrateurs systèmes et réseaux
- Auditeurs informatiques

#### Pré-requis

- Connaissances techniques approfondies en réseau et système (OS)

### Objectifs

- Comprendre les menaces cybernétiques actuelles Savoir comment se préparé Apprendre à réagir adéquatement

### Programme

#### Threat LandScape

- Overview of current threats, Dropping, Exploit, communication tricks ; DGA, FastFlux

#### Reactions Preparation ( detection, reaction, lessons learned et on recommence)

- Reaction preparation
- 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)

#### How to face External Threat

- Vpn Abuse : Detections tricks
- Phishing : Detections tricks, response, take down
- DDos : Detection basics, Mitigation
- Data Thief : Detections basics

#### How to face Internal threat

- Understand Threats installation

#### Windows Internals

- Review of MS Windows architecture
- UserLand/Kerneland séparation

- Threads/process/fibers
- Process migration/Injection

#### Exploitations

- Current Vulnerability Buffer overflow/UAF
- Common exploitation technics ROP/Heapspray
- Exploit packs
- Forensic possibilities

#### Detect and find threats

- Office files and script droppers
- How office documents are used
- VBA Document analyse

#### JS analysis

- Obfuscations
- Tools for unobfuscation

#### Evidences collection

- How to take evidences (Art of memory and Disk dump)
- Sandbox (usage, beneficts and restrictions)
- Tooling (Volatility, Sysinternals, Detection tools)

#### Appropriate actions to appropriate threads

- Ransomwares (Detection, Reaction )
- Common Malwares (Detection, Reaction)
- Rats (Detection, Reaction)
- Website breaches (Detection Reaction)

### Modalités

- **Type d'action** :Acquisition des connaissances
- **Moyens de la formation** :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- **Modalités pédagogiques** :Exposés – Cas pratiques – Synthèse
- **Validation** :Exercices de validation – Attestation de stages