INVESTIGATION NUMÉRIQUE - Durée 35h

OBJECTIFS

- Appréhender la méthode d'investigation et savoir consolider un plan de réponse à incident

PUBLIC CIBLE

- Administrateurs système,
- Développeurs

PRE-REQUIS

- Base TCP/IP, OS Windows / Linux et programmation

PROGRAMME

Fondamentaux de l'investigation numérique

- Découverte du monde de l'investigation numérique
- Méthodologie d'investigation légale

Collecte de données, timeline, analyse et rapport

- Données sur disque
- RAM
- Fichier d'hibernation

Artefacts $MFT, registre, évènements

- Clés de registre
- Shellbag
- Prefetch
- Evènement Windows

Forensic web

- Social engineering
- Anonymat, Tor
- Dark web et Cloaking

Forensic réseaux

- Investigation légale dans les réseaux
- Utilisation des journaux de logs à des fins d'investigation
- Enquêter sur le traffic réseau
- Enquêter sur les attaques Wireless

Forensic Windows/Linux

- Processus de lancement des systèmes
- Investigation légale dans Windows
- Analyse du cache, cookie et historique de navigation, historique des évènements
- Investigation légale Linux
- Acquisition de données et duplication
- Outils d'investigation légale
- Investigation légale
- Investigations légales utilisant Encase

Cas pratique

- Etude et protection après incident sur les systèmes d'exploitation Windows
- Rédaction d'un plan de réponse à incident

MOYENS TECHNIQUES ET HUMAINS :

- Intervenant : Formateur Professionnel
- Mobilisation des outils et auxiliaires utiles : paperboard, vidéoprojecteur…
- Possibilité de mettre à disposition des PC portables pour les stagiaires

METHODES PEDAGOGIQUES MOBILISEES :

- Alternance de méthodes affirmatives, interrogatives et actives
- Ressources de type formatives, évaluatives, de synthèses, de soutien, de mémorisation…
- Utilisation de Padlet

MODALITES D'EVALUATION :

- Des acquis
  - Fiche de renseignements en amont et questions
  - Evaluations formatives réalisées à l'aide de grilles critériées ;
  - Attestation de fin de formation mentionnant l'atteinte des objectifs de la formation
  - Evaluation différée
- Evaluation satisfaction
- Rédaction d'un bilan d'action remis au commanditaire en cas de formation intra-entreprise