Management de la sécurité de l'information

Initiation à la Cyber criminalistique

Vous allez apprendre à

- Comprendre les principes fondamentaux de la criminalistique numérique (computer forensics).
- Connaître le cycle complet d'investigation numérique : acquisition, analyse, documentation.
- Identifier les artefacts critiques sur systèmes Windows, Linux, Mac et réseaux.
- Découvrir les outils et bonnes pratiques pour préserver la preuve numérique.
- Appréhender les techniques d'investigation sur les emails, malwares et web/dark web.
- Maîtriser les bases de la conformité, de la traçabilité et des standards de la preuve.

Public visé

- Professionnels IT, analystes sécurité, administrateurs systèmes/réseaux.
- Équipes SOC, CERT/CSIRT, débutants en investigation numérique.
- Étudiants et professionnels en reconversion vers la cybersécurité technique.

Les objectifs de la formation

À la fin de la journée, les participants sauront :

- Identifier les principales étapes d'une investigation numérique conforme.
- Détecter et extraire des preuves numériques sur systèmes, réseaux et environnements web.
- Comprendre comment les données sont stockées, copiées, dissimulées ou effacées.
- Appliquer les bonnes pratiques d'acquisition et de préservation de preuve.
- Utiliser des outils de base pour collecter, examiner et documenter des incidents.

Les prérequis de la formation

- Notions de base en systèmes d'exploitation et réseaux.
- Une curiosité pour la cybersécurité technique (niveau débutant à intermédiaire).

Programme de la formation

- **Accueil & contexte : rôle de l'investigation numérique dans la cybersécurité**
  - Module 1 : Introduction à la criminalistique numérique & processus d'investigation
  - Module 2 : Systèmes de fichiers, disques & acquisition des données
  - Module 3 : Analyse de systèmes Windows, Linux & Mac OS
  - Module 4 : Investigation sur réseaux, emails et incidents web
  - Module 5 : Forensics avancé : anti-forensics, dark web et malwares
- **Atelier pratique guidé : scénario d'investigation avec artefacts**
- **Débrief & QCM d'évaluation**