S'initier à l'analyse inforensique

En cas de piratage informatique ou d'incident de sécurité majeur, l'analyse inforensique s'impose. Appelée aussi analyse post-mortem, elle demande beaucoup de rigueur et de précision car les preuves récoltées sont parfois fragiles et volatiles.

Durée
5 jours - 35 heures

Prix inter
3500 €HT

Prochaines dates
8 au 12 octobre 2018
10 au 14 décembre 2018

Méthodes pédagogiques
12 participants maximum. Un poste par personne. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de l'analyse inforensique.

Après cette formation, vous pouvez suivre la formation Perfectionner son analyse inforensique.

Compétences visées

- Mettre en œuvre une analyse inforensique
- Récolter des preuves utilisables dans un cadre juridique

Objectifs pédagogiques

- Identifier les méthodes d'analyse inforensique
- Créer des scénarios d'investigation
- Trier et analyser les informations récoltées
- Rendre une synthèse de son analyse

Public

Toute personne souhaitant se lancer dans l'analyse inforensique

Prérequis

Avoir des connaissances informatiques est nécessaire.

Programme

Définir l'inforensique

- Expliquer l'inforensique
- Identifier le périmètre de l'investigation
- Définir le "First Responder" et sa méthode

Mettre en œuvre une analyse inforensique

- Identifier les éléments à analyser : les disques dur, leurs systèmes de fichiers, la mémoire
- Récupérer des données persistantes et volatiles
- Gérer des supports chiffrés
- Rechercher des données supprimées

Identifier les données des registres Windows

- Définir les structures de registres Windows
- Analyser les journaux d'événements

Mettre en place des scénarios d'investigation

- Identifier les accès à des contenus sécurisés
- Repérer des traces de manipulation de fichiers et de dossiers
- Vérifier la sécurité des réseaux
- Vérifier la sécurité des logiciels
- Étudier la sensibilisation des personnes à l'ingénierie sociale
- Repérer les trous de sécurité via le Web
- Identifier les principaux artefacts des systèmes OSX et Linux

Réaliser de l'inforensique réseau

- Identifier les différents types de preuves réseaux
- Lister les évènements pouvant être trouvés
- Analyser les journaux DNS, DHCP, Proxy, pare-feu
- Analyser des paquets
- Repérer les canaux de contrôle et d'exfiltration

Analyse chronologique

- Créer et analyser une timeline des événements
- Comparer des scénarios d'intrusion