

## Lutte contre la cybercriminalité : Travaux Pratiques - 4 jours

### Analyse des systèmes Windows

*formation 536*

- Vous apprendrez à**
- Mettre en oeuvre, dans le cadre de l'investigation numérique, une stratégie de réponse aux incidents
  - Mener une investigation réussie de "A à Z" à partir de l'incident
  - Analyser le disque et récupérer les fichiers supprimés
  - Identifier les techniques de dissimulation d'informations
  - Reconstruire l'activité d'un utilisateur à partir des courriels, des fichiers Internet temporaires et des données en cache
  - Accéder à l'intégrité de la mémoire système et de l'architecture des processus afin de révéler la présence de code malicieux

**Objectif** Sauriez-vous quoi faire si la sécurité de votre entreprise était en péril ? Face à la recrudescence des menaces de cybercriminalité, il existe des mesures que vous pouvez prendre pour protéger votre entreprise. Dans ce cours, vous mettrez en application les dernières techniques d'investigation d'un système informatique Windows, afin de révéler toute activité illicite et de récupérer les données perdues. Chaque crime laisse des indices derrière lui. En utilisant les bons outils, vous pourrez répondre et contrer les menaces de manière efficace.

**À qui s'adresse cette formation** Aux administrateurs système et à tous ceux qui doivent faire face à des incidents de sécurité. La connaissance des PC fonctionnant sous Windows (matériel, logiciels du système d'exploitation), du niveau de la formation.

**Travaux pratiques** Vous acquerez une expérience pratique de l'utilisation d'outils d'investigation sur des systèmes Windows. Les exercices comprennent:

- Optimisation des logiciels de gestion de cas
- Utilisation des outils d'investigation
- Imageur numérique
- Dissimulation et découverte de preuves potentielles
- Application des techniques de stéganographie
- Manipulation des flux de données superposées
- Découverte d'informations dans des fichiers corrompus
- Investigation du courriel
- Reconstitution de l'activité du navigateur et du serveur Web
- Mise en œuvre d'une surveillance avec un accès à distance et enregistrement des frappes clavier
- Configuration d'outils pour détecter un kit au niveau racine

## Lutte contre la cybercriminalité : Travaux Pratiques - 4 jours

### Analyse des systèmes Windows *formation 536*

#### Introduction à l'investigation numérique

- Réponse aux incidents
- Application de techniques d'investigation
- Différence entre l'activité normale de l'entreprise et l'activité criminelle

#### Investigation préliminaire

##### Démarche de réponse aux incidents

- Connaissance des politiques de votre entreprise
- Minimisation de l'impact sur votre entreprise

##### Cycle de vie des incidents

- Analyse des incidents
- Capture d'informations volatiles

#### Maîtrise de l'investigation

##### Collecte de preuves numériques

- Faire valoir ses droits devant la justice
- Maintenance de l'intégrité du processus
- Atouts de l'équipe d'investigation

##### Aspects juridiques de l'acquisition de preuves

- Sécurisation et étude de la scène du crime
- Constitution d'un recueil de preuves

#### Analyse du disque

##### Opérations d'investigation en laboratoire

- Acquisition d'une image physique du disque
- Activation du blocage en écriture
- Mise en place d'une ligne de conduite
- Protection physique du média

##### Structure du disque et techniques de récupération

- Composants de la géométrie du disque
- Inspection des architectures système des fichiers Windows
- Localisation et restauration du contenu supprimé

#### Techniques de dissimulation des informations

##### Découverte des informations cachées

- Analyse des flux de données superposées
- Exécution de code à partir de divers flux
- Outils et concepts de stéganographie
- Détection de la stéganographie
- Analyse des espaces libres

##### Exploration du contenu d'en-tête et des fichiers corrompus

- Combinaison de fichiers
- Enchaînement de fichiers multiples
- Analyse des dates de fichiers

#### Examen du courriel

##### Investigation du client de messagerie

- Interprétation des en-têtes de courriels
- Récupération des courriels supprimés

##### Validation des informations des en-têtes

- Détection des courriels pastiches
- Vérification du routage des courriels

#### Trace des accès Internet

##### Inspection de l'historique et du cache

- Exploration des fichiers temporaires Internet
- Recherche du stockage de cookies
- Reconstruction de l'historique du navigateur
- Accès aux navigateurs avec des caractéristiques illégales
- Analyse du navigateur actualisée

##### Audit de la navigation sur Internet

- Suivi de l'activité de l'utilisateur
- Repérage des utilisations non autorisées

#### Inspection de la mémoire en temps réel

##### Comparaison de l'architecture des processus

- Identification de la mémoire utilisateur et de la mémoire du noyau
- Inspection des threads
- Étude des DLL ou des pilotes illicites

##### Méthodes d'analyse avancées

- Évaluation des processus avec WMI (Windows Management Instrumentation)
- Navigation dans les arborescences

##### Audit des services et processus

- Investigation de la table de processus
- Découverte de preuves dans la base de registre
- Déploiement d'un kit au niveau racine

#### Techniques de surveillance furtive

- Enregistrement des frappes clavier
- Observation en temps réel des postes distants
- Contrôle de l'accès Internet