EduGroupe
Accompagner pour réussir

Sécurité : Analyse inforensique Windows

Référence : **SECAIW** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- Avoir de solides bases en sécurité des systèmes d'information

Profil des stagiaires

- 1-Personnes souhaitant apprendre à réaliser des investigations numériques
- 2-Personnes souhaitant se lancer dans l'inforensique
- 3-Administrateurs système Windows
- 4-Experts de justice en informatique

Objectifs

- Gérer une investigation numérique sur un ordinateur Windows
- Avoir les bases de l'analyse numérique sur un serveur Web
- Acquérir les médias contenant l'information
- Trier les informations pertinentes et les analyser
- Utiliser les logiciels d'investigation numérique
- Maîtriser le processus de réponse à incident

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Inforensique

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Présentation de l'inforensique

- Présentation de l'inforensique
- Périmètre de l'investigation
- Trousse à outil
- Méthodologie « First Responder »
- Analyse Post-mortem
- Disques durs
- Introduction aux systèmes de fichiers
- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows : Utilisateurs
- Analyse des journaux
- Évènements / antivirus / autres logiciels

2. Scénario d'investigation

- Téléchargement/Accès à des contenus confidentiels
- Exécution de programmes
- Traces de manipulation de fichiers et de dossiers
- Fichiers supprimés et espace non alloué
- Carving
- Géolocalisation
- Photographies (données Exifs)
- Points d'accès WiFi
- HTML5
- Exfiltration d'informations
- Périphérique USB
- Courriels
- Journaux SMTP : Acquisition coté serveur
- Utilisateurs abusés par des logiciels malveillants

3. Interaction sur Internet

- Utilisation des Navigateurs Internet
- IE/Edge / Firefox
- Office 365
- Sharepoint
- Traces sur les AD Windows
- Présentation des principaux artefacts
- Bases de l'analyse de la RAM : Conversion des hyberfiles.sys

4. Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux »
- Les bases de l'inforensique sur un serveur Linux : Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d'une frise chronologique du système de fichier

5. Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts
- Exemple d'outil d'interrogation de gros volume de données

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.