ANALYSE INFORENSIQUE WINDOWS

Public	Administrateur / Ingénieur système et réseau Analyste SOC / Inforensique Personnes souhaitant se lancer dans l'inforensique
Durée	3 jours - 21 heures
Pré-requis	Bonnes connaissances dans les systèmes Windows, en réseau et en cybersecurité
Objectifs	Savoir réaliser une investigation numérique sur un ordinateur Windows Pouvoir utiliser les outils d'investigation Être capable de collecter et préserver l'intégrité des preuves
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. INTRODUCTION À WINDOWS ET À LA CYBERSÉCURITÉ

- OS Windows : les chiffres
- Les vulnérabilités Windows
- Les menaces les plus communes
- Inforensique numérique Windows
- La base de registre

2. INTRODUCTION À L'ANALYSE INFORENSIQUE

- Définition et terminologie
- Les objectifs du inforensique numérique
- Le processus d'investigation des incidents
- La chaîne de traçabilité

3. ANALYSE INFORENSIQUE RÉSEAU

- Définition et terminologie
- Les types de collectes réseaux
- Les outils d'analyse réseau
- Wireshark dans un cadre d'investigation
- Analyse de flux réseaux malveillant

4. ANALYSE INFORENSIQUE DES TRACES

- Définition et terminologie
- La collecte des traces
- Les outils d'analyse des traces
- Les événements Windows
- Analyse d'événement suite à une activité malveillante

5. ANALYSE INFORENSIQUE MÉMOIRE

- Définition et terminologie
- La collecte de la mémoire
- Les outils d'analyse mémoire
- Maitrise de volatility
- Analyse mémoire sur système

6. ANALYSE INFORENSIQUE DU SYSTÈME DE FICHIERS

- Définition et terminologie
- Système de fichiers Windows
- La collecte du stockage de masse
- Les outils
- Analyse d'activité malveillante sur système Windows

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation