Certified Windows Forensics Manager

Référence : **SECCWFM** Durée : **5 jours** Certification : **Certified Windows Forensic Manager**

CONNAISSANCES PREALABLES

• Connaissance du système Windows. • Connaissance réseaux et modèle OSI. • Les principes de réponse à Incident.

PROFIL DES STAGIAIRES

• Analystes de Cyber intelligence et analystes de données électroniques Professionnels souhaitant approfondir leurs connaissances en analyse des investigations informatiques. • Professionnels de la cybersécurité. • Spécialistes des TI.

OBJECTIFS

• Comprendre les concepts et référentiels du forensique. • Appréhender une analyse sur les environnements Windows. • Connaissance des outils et source de veille.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Inforensique

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

Introduction Forensique et Windows

• Introduction : Historique de l'Inforensique - Méthodologie et référentiel du forensique - Processus et gestion des incidents - Les preuves et leurs traitements - Processus et préparation de l'analyse
• Les lignes directrices de l'analyse d'un système Window
• Présentation du système Windows : Fonctionnement systèmes - Les composants

Collecte Live et acquisition

• Réponse initiale – Live – La trousse à outils et les précautions : Création d'une clé USB d'analyse Windows
• Démarrage de l'investigation - Création d'un dossier : Collecte des données volatiles - Quoi collecter ? - Collecte des données volatiles - Les éléments importants
• Les bases de l'acquisition mémoire
• Recommandation d'acquisition du disque :Acquisition du disque - Présentation du système de fichier Windows (NTFS - MFT)

Analyse mémoire

• Traitement du fichier mémoire : Présentation Volatility - Création de profile - Information processus, Mappage des processus - Information de base avec volatility - Information réseau

Analyse du registre

- Compréhension de la base de registre : Extraction des ruches - Ruche système - Ruche software - Ruche utilisateur

Analyse de disque

- Traitement du disque : Analyse corbeille - Extraction des informations utilisateurs - Analyse du navigateur - Analyse des logs - Analyse du système de fichier et TimeLine - Analyse du preftech

- Introduction à l'analyse des malwares PE : Les différents types d'analyses - L'analyse statique - L'analyse dynamique - L'analyse statique avancée de malware - L'analyse dynamique avancée - Les techniques d'offuscation - Technique de reporting