EduGroupe
Accompagner pour réussir

Certified Windows Forensics Manager

Référence : **SECCWFM** Durée : **5 jours (35 heures)** Certification : **Certified Windows Forensic Manager**

Connaissances préalables

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

Profil des stagiaires

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

2. 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)

3. Analyse mémoire

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

4. Analyse du registre

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

5. 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

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.