

- *Connaître les concepts et méthodes de l'analyse fresque propre aux systèmes Windows*
- *Savoir mener une analyse technique poussée les environnements Windows*
- *Maîtriser le fonctionnement des outils d'investigation*
- *Savoir organiser une veille technologique*
- *Préparer et passer l'examen de certification « CWFM, Certified Windows Forensics Manager » du PECB*

5**Prix : 3?450 € € / HT****OUTILS PÉDAGOGIQUES****PUBLIC VISÉ**

- 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

MODALITÉS D'ÉVALUATION**MODALITÉS DE FINANCEMENT****MODALITÉS ET DÉLAIS D'ACCÈS****OBJECTIFS PÉDAGOGIQUES****ACCESSIBILITÉ****LES POINTS FORTS DE LA FORMATION****PRÉ-REQUIS**

- Connaissance pratique des systèmes Windows, des réseaux et du modèle OSI
- Tous les candidats devront présenter une carte d'identité valide avec une photo lors du passage de l'examen

MODALITÉS ET DÉLAIS D'ACCÈS**ATTESTATION OBTENUE****EFFECTIF DE LA FORMATION****CERTIFICATION****MODALITÉ PÉDAGOGIQUE**

Cours dispensé en mode présentiel avec une alternance d'apports théoriques et méthodologiques, et de mises en situations pratiques

PROCHAINES SESSIONS

Nous consulter.
Nous consulter.
Nous consulter.

PROGRAMMES DE CWFM, CERTIFIED WINDOWS FORENSICS MANAGER**INTRODUCTION À LA FORENSIQUE ET WINDOWS**

- Historique de l'infoforensique
- 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 Windows
- Fonctionnement des systèmes Windows
- Les composants de Windows

COLLECTE LIVE ET ACQUISITION DES DONNÉES DU DISQUE

- La trousse à outils et les précautions à prendre dans le cas d'une réponse initiale (en live) à un incident de sécurité : Création d'une clé USB d'analyse Windows
- Démarrage de l'investigation : Création d'un dossier, Collecte de données volatiles (Quoi collecter, les éléments importants,...)
- Les bases de l'acquisition mémoire
- Recommandations d'acquisition du disque
- Acquisition du disque
- Présentation du système de fichiers Windows : NTFS, MFT
- Montage de disque

ANALYSE DE LA 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

- Présentation de la base de registre
- Extraction des ruches
- Analyse de la ruche système
- Analyse de la ruche software
- Analyse de la ruche utilisateur

ANALYSE DE DISQUES

- Traitement du disque : Analyse de la corbeille, extraction des informations utilisateurs, analyse du navigateur, analyse des logs, analyse du système de fichiers et de la TimeLine et analyse du preftech

EXAMEN PECB CERTIFIED WINDOWS FORENSICS MANAGER

- Révision des concepts en vue de la certification
- Examen blanc
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- Les candidats sont autorisés à utiliser les supports de cours mais aussi les notes qu'ils auront prises
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétences suivants : Domaine 1 : Connaissance des référentiels et des méthodologies du forensique global – Domaine 2 : Investigation et recommandation dans les environnements Windows – Domaine 3 : Utilisation des outils à des fins d'analyse – Domaine 4 : Compréhension de la méthodologie