

- *Appréhender les référentiels liés à la réponse à incident*
- *Connaître les outils utiles pour la réponse à incident*
- *Comprendre le cycle de la réponse à incident*
- *Comprendre les points clés de la l'investigation forensique*
- *Préparer et passer l'examen de certification « CIHM, Certified Incident Handling Manager » du PECB*

5

Prix : € / HT

OUTILS PÉDAGOGIQUES**PUBLIC VISÉ**

Tout public

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

- Connaissance de base des systèmes Linux, Windows
- Connaissance des réseaux et du modèle OSI
- Connaissance simple des éléments de sécurité (analyse de logs, principe des attaques réseaux,...)
- 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 CIHM, CERTIFIED INCIDENT HANDLING MANAGER**INTRODUCTION À LA RÉPONSE À INCIDENT**

- Qu'est ce que la réponse à incident

- Le contexte de la réponse à incident
- Les normes et référentiels

LE CYCLE DE RÉPONSE À INCIDENT

- Préparation
- Identification
- Confinement
- Éradication
- Récupération
- Problèmes légaux

PRÉPARATION ET IDENTIFICATION

- Les différents éléments de la réponse à incident : Alertes et évènements
- Le lancement d'une intervention
- Les composants de la réponse à incident : NIDPS, HIDPS, journaux d'évènements – SIEM

CONFINEMENT ET ÉRADICATION

- Les principes de confinement : à court terme, à long terme
- Le forensique
- Création de e système d'investigation : étude de la trousse à outil, analyse Live, analyse de la mémoire, analyse de disque, Rétro-ingénierie
- Création d'indicateur de compromission
- Mise en oeuvre de l'indicateur dans les outils d'identification
- Rédaction des procédures
- Éradication

RÉCUPÉRATION

- Détermination de la portée de l'attaque
- Restauration des sauvegardes
- Organisation des tables rondes pour tirer les leçons de l'expérience
- Résumé de la réponse à l'incident : Analyse complète du cycle : Détection dans les outils d'identification, confinement du système infecté, analyse complète du système, création d'indicateurs, mise en oeuvre des indicateurs dans les outils d'identification, détection de l'attaque

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 : Comprendre et savoir analyser les éléments phares de la réponse à incident (NIDPS, Logs, Analyse du système – Domaine 2 : Connaissance et étude des référentiels – Domaine 3 : Mener une recherche et analyse d'une application – Domaine 4 : Connaissance et étude des référentiels – Domaine 5 : Généralités sur les attaques d'un SI – Domaine 6 : Configuration d'indicateurs dans les outils d'identification