Certified Incident Handling Manager

Référence : **SECCIHM** Durée : **5 jours** Certification : **PECB**

CONNAISSANCES PREALABLES

• 1-Connaissance de base des systèmes Linux, Windows. • 2-Connaissance des réseaux et du modèle OSI. • 3-Connaissance simple des éléments de sécurité (analyse de logs, principe des attaques réseaux,...). • 4-Tous les candidats devront présenter une carte d'identité valide avec une photo lors du passage de l'examen.

PROFIL DES STAGIAIRES

• Professionnels de la cybersécurité. • Spécialistes des TI.

OBJECTIFS

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

CERTIFICATION PREPAREE

PECB Certified Incident Handling Manager

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 Management de la sécurité

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 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 œuvre 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
- Résume 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 œuvre des indicateurs dans les outils d’identification, détection de l’attaque

Examen PECB Certified Incident Handling 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