

Certified Lead Forensics Examiner

Référence : SECCLFE

Durée : 5 jours

Certification : PECB

Code CPF : RS3717

CONNAISSANCES PREALABLES

- Connaissance du système Linux/windows/mobile.
- Connaissance réseaux et modèle OSI.
- Les principes de réponse à Incident.

PROFIL DES STAGIAIRES

- Analyste de données.
- Analyste de media électronique.
- Consultant.
- Membre d'équipe sécurité.
- Spécialiste en recherche et récupération de preuves informatiques.
- Spécialiste investigation informatique.

OBJECTIFS

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

CERTIFICATION PREPAREE

- PECB Certified Lead Computer Forensics Examiner. Pour en savoir plus sur cette certification [cliquez ici](#) et accédez aux informations complètes fournies par France Compétences. Pour connaître tous les détails concernant les prérequis relatifs au passage de l'examen de certification en ligne, nous vous invitons à [cliquer ici](#) pour accéder à la documentation officielle du certificateur

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 Infoforensique

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

Présentation et méthodologie

- Objectifs et structure du cours
- Introduction aux Forensiques
- Méthodologie et référentiel de l'infoforensique
- Processus et gestion des incidents
- Les preuves et leurs traitements
- Processus d'analyse & préparation de l'analyse
- Réponse initiale – La trousse à outils

Réponse initiale et acquisition des preuves

- Réponse initiale – Préparation et analyse : Linux Collecte informations, memdump - Windows Collecte Information, memdump - Mobile (Android, iOS)

- Présentation des systèmes de fichiers
- Duplication – Précautions et Méthodologie
- Duplications d'images de disque

Montage des disques et analyses

- Préparation à l'analyse du système de fichiers
- Analyse des données du système de fichiers – Windows
- Analyse des données du système de fichiers – UNIX/Linux
- Analyse des données du système de fichiers – Mobilité
- Analyse : Le cas du Cloud
- Analyse des emails

- Analyse du web

Analyse Réseau

- Rappel OSI
- Utilisation de Wireshark
- Les outils dans wireshark
- Analyse de flux malveillant
- Création de profil forensic

Document et Reporting

Certification PECB Certified Lead

Computer Forensics Examiner

- Révision des concepts en vue de la certification
- Examen blanc
- Passage de l'examen écrit de certification en français qui consiste à répondre à 12 questions en 3 heures