CERTIFICATION EN GESTION DES INVESTIGATIONS LEGALE INFORMATIQUE (LEAD FORENSICS EXAMINER)

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1003

MAITRISER LA MISE EN OEUVRE DES PROCESSUS D'INVESTIGATION LEGALE INFORMATIQUE

RÉSUMÉ

Ce cours intensif de 5 jours permet aux participants de développer l'expertise nécessaire à la maitrise des processus d'investigation légale informatique, comme spécifié par la certification CLFE (Certified Forensic Lead Examiner). Les participants vont acquérir une compréhension des concepts de base de l'investigation informatique, basé sur les bonnes pratiques à mettre en œuvre pour préserver les preuves ainsi que le processus analytique associé. La certification CLFE se focalise sur les compétences requises pour acquérir et analyser les données collectées sur des systèmes Windows, Mac OS X, Linux, ainsi que sur les appareils mobiles.

CURSUS DETAILLE

DURÉE: 5 JOURS

JOUR 1
Introduction aux principes scientifiques spécifiques à l'investigation informatique

- Principes scientifiques spécifiques à l'investigation informatique
- Introduction à l'approche de l'investigation informatique
- Analyse et mise en œuvre des opérations d'analyse
- Préparation et exécution des procédures d'investigation

JOUR 2
Structure des ordinateurs et des systèmes d'exploitation

- Identification and sélection des composants d'un ordinateur
- Identification et sélection des périphériques et autres composants
- Compréhension des systèmes d 'exploitation
- Extraction et analyse des structures de fichier

JOUR 3
Investigation réseau et des appareils mobiles

- Comprendre les réseaux, le cloud et les environnements virtuel
- Méthodes génériques pour l'extraction de données dans un environnement virtuel
- Examen d'un téléphone mobile ou d'une tablette
- Stockage des informations sur les appareils mobiles

JOUR 4
Outils et méthodologies d'investigation

- Enumération et examen des composants matériels et logiciels des ordinateurs
- Choix et test des technologies d'investigation
- Analyse et sélection des procédures adaptées pour les opérations d'investigation
- Découverte, documentation et retour des preuves sur site
- Analyse et prise en compte du contexte

JOUR 5 ANSI Accredited Certification Exam

QUI EST CONCERNE ?

- Spécialiste en investigation informatique
- Analystes de données
- Spécialistes en recherche et récupération de preuves informatique
- Professionnels travaillant dans le domaine de l'investigation informatique
- Membres d'équipe sécurité
- Consultants
- Professionnels dans l'analyse de media électronique

OBJECTIFS DU COURS

- S'assurer que le CLFE est en mesure de protéger sa crédibilité et protéger l'intégrité des medias analysés tout au long des opérations d'investigation
- S'assurer que le CLFE peut mener les opérations d'investigation ainsi que la démarche à adopter pour atteindre les objectifs attendus
- S'assurer que le CLFE peut opérer en toute sécurité sur les ordinateurs, extraire ou installer les périphériques ou composants nécessaires, identifier la présence de certains ports ou éventuelle présence de media contenant de l'information à examiner
- S'assurer que le CLFE a le savoir nécessaire pour trouver l'information pertinente sur un media ou sur une image bit-à-bit de celui-ci, que celle-ci soit présente, effacée ou cachée par le système d'exploitation ou par l'utilisateur
- S'assurer que le CLFE peut conduire une investigation légale informatique, qui préserve les preuves et les rend recevables par un tribunal, dans un réseau, dans le cloud ou dans un environnement virtuel
- S'assurer que le CLFE peut conduire une investigation de base sur un smartphone ou une tablette.
- S'assurer que le CLFE peut utiliser de manière efficace les outils d'investigation (logiciels, matériels) sur le terrain
- S'assurer que le CLFE est en mesure d'expliquer et de justifier comment les données pertinentes ont été extraites, classifiée, identifiées et gérées de manière légale tout au long de la procédure

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1003

www.pecb.org/accreditation

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1003

www.pecb.org/accreditation

EXAMEN

- L'examen "Certified ISO/IEC 27005 Risk Manager" " est pleinement conforme avec les exigences du programme d'examen et de certification de PECB (Examination and Certification Program – ECP). L'examen couvre les domaines suivants:

1 DOMAINE 1: PRINCIPES SCIENTIFIQUES SPÉCIFIQUES À L'INVESTIGATION INFORMATIQUE

Objectif principal: S'assurer que le CLFE est en mesure de protéger sa crédibilité et protéger l'intégrité des medias analysés tout au long des opérations d'investigation

2 DOMAIN 2: PRINCIPES FONDAMENTAUX DE L'INVESTIGATION INFORMATIQUE

Objectif principal: S'assurer que le CLFE peut mener les opérations d'investigation ainsi que la démarche à adopter pour atteindre les objectifs attendus

3 DOMAINE 3: STRUCTURE DES ORDINATEURS

Objectif principal: S'assurer que le CLFE peut opérer en toute sécurité sur les ordinateurs, extraire ou installer les périphériques ou composants nécessaires, identifier la présence de certains ports ou éventuelle présence de media contenant de l'information à examiner

4 DOMAINE 4: SYSTÈMES D'EXPLOITATION ET STRUCTURES DE FICHIER

Objectif principal: S'assurer que le CLFE a le savoir nécessaire pour trouver l'information pertinente sur un media ou sur une image bit-à-bit de celui-ci, que celle-ci soit présente, effacée ou cachée par le système d'exploitation ou par l'utilisateur

5 DOMAINE 5: INVESTIGATION RÉSEAU, DANS LE CLOUD OU DANS LES ENVIRONNEMENTS VIRTUELS

Objectif principal: S'assurer que le CLFE peut conduire une investigation légale informatique, qui préserve les preuves et les rend recevables par un tribunal, dans un réseau, dans le cloud ou dans un environnement virtuel

6 DOMAINE 6: INVESTIGATION RÉSEAU ET DES APPAREILS MOBILES

Objectif principal: S'assurer que le CLFE peut conduire une investigation de base sur un smartphone ou une tablette.

7 DOMAINE 7: OUTILS ET MÉTHODOLOGIES D'INVESTIGATION

Objectif principal: S'assurer que le CLFE peut utiliser de manière efficace les outils d'investigation (logiciels, matériels) sur le terrain

8 DOMAINE 8: EXAMEN, ACQUISITION ET PRÉSERVATION DES PREUVES ÉLECTRONIQUES

Main Objective: S'assurer que le CLFE est en mesure d'expliquer et de justifier comment les données pertinentes ont été extraites, classifiée, identifiées et gérées de manière légale tout au long de la procédure

- L'examen "Certified Lead Forensics Examiner exam est disponible en différents langages : Anglais, Français, Espagnol et Portuguais.
- Durée: 3 heures
- Pour plus d'information: www.pecb.org

CERTIFICATION

- Un certificat "Certified Lead Forensics Examiner" est délivré aux participants qui auront réussi l'examen et qui remplissent l'ensemble des autres exigences relatives au niveau de qualification choisi :

Certification	Examen	Professional Experience	Formation	Autres exigences
Certified Lead Forensics Examiner	Examen Certified Lead Forensics Examiner	**Deux ans** Dont un an en investigation informatique	Formation supérieure	Signer le code d'éthique PECB

INFORMATIONS GENERALES

- Les frais de certification sont inclus dans le prix de l'examen
- Un manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques est fourni aux participants
- À l'issue de la formation, un certificat de participation de 31 crédits CPD (Continuing Professional Development) est délivré aux participants
- En cas d'échec, les participants peuvent repasser l'examen sans frais, sous certaines conditions.

Pour plus d'informations,
veuillez nous contacter à info@pecb.org

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1003

www.pecb.org/accreditation