Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Lead Forensics Examiner : l'informatique judiciaire

Date et durée

Code formation : CLFE
Durée : 5 jours
Nombre d'heures : 31 heures

Sessions
Classe Virtuelle le 24 mai 2021 (212004)

Description

Le **computer forensics** ou l'**investigation numérique légale** est un ensemble de méthodes et techniques visant à identifier et collecter des preuves numériques sur un réseau ou un appareil informatique à la demande d'une instance judiciaire. L'examinateur est la personne en charge de **mener ou de superviser** l'ensemble des procédures de l'investigation au sein d'un réseau informatique d'une organisation.
La **formation Lead Forensics Examiner** vous apprendra à comprendre et maîtriser les opérations d'investigation informatique dans un cadre légal avec les meilleures pratiques d'exploitation et de protection des preuves. Elle vous préparera également à l'examen de certification **PECB Certified Lead Forensics Examiner**, afin de déterminer votre aptitude à conduire une investigation informatique légale.
Cette formation présente aussi de **nombreux avantages applicables** aux organisations de toute taille dans le domaine de la technologie tels que :

- une gestion renforcée de la sécurité et une meilleure réactivité face aux incidents ;
- une capacité à comprendre et tracer l'origine des incidents et l'implication des utilisateurs ;
- un avantage concurrentiel ;
- une conformité à la loi et aux règlementations en vigueur.

Téléchargez le guide Lead Forensics Examiner

Objectifs

A l'issue de la formation **Lead Forensics Examiner**, vous atteindrez les objectifs suivants :

- comprendre les enjeux d'une investigation informatique et la responsabilité du Lead Computer Forensics Examiner ;
- savoir les objectifs, normes et méthodologies communes d'un examen des médias électroniques ;
- connaître la séquence correcte des étapes lors d'une investigation légale numérique et d'une enquête sur un incident informatique ;
- identifier les outils libres et les outils communs employés lors d'une enquête d'incident et d'une opération judiciaire numérique ;
- développer les compétences indispensables à la planification et l'exécution d'une opération informatique judiciaire ;
- savoir réaliser la mise en œuvre et le maintien d'un réseau de sécurité protégeant les preuves ;
- réussir l'examen et obtenir votre certification PECB Certified Lead Computer Forensics Examiner.

Points forts

Travaux pratiques basés sur des cas réels avec une documentation de 450 pages; 31 crédits FPC ; Examen de

certification compris dans le prix de la formation ; En cas d'échec, repassez-le sans frais dans les 12 mois.

Certification

L'examen **PECB Certified Lead Computer Forensics Examiner** remplit les exigences relatives au programme d'examen et de certification de PECB. Il couvre les domaines de compétences suivants :

- les principes et concepts fondamentaux de l'investigation informatique ;
- les meilleures pratiques en investigation informatique ;
- les exigences relatives au laboratoire légal numérique ;
- les systèmes d'exploitation et la structure du système de fichiers ;
- les appareils mobiles ;
- l'enquête sur la criminalité informatique et examen forensique ;
- le maintien de la chaîne des preuves.

Vous disposez de 3 heures pour passer l'examen PECB Certified Lead Computer Forensics Examiner. Suite au succès de l'examen et à condition de remplir certaines exigences, vous pourrez demander l'une des certifications suivantes :

- **Certified Provisional Computer Forensics Examiner :** aucune expérience nécessaire, signer le code de déontologie PECB ;
- **Certified Computer Forensics Examiner :** 2 ans d'expérience pro. dont 1 an en informatique judiciaire, 200 heures d'activités dans le domaine, signer le code de déontologie PECB ;
- **Certified Computer Lead Forensics Examiner :** 5 ans d'expérience pro. dont 2 en informatique judiciaire, 300 heures d'activités dans le domaine, signer le code de déontologie PECB.

Pour en savoir plus sur les modalités, consulter le règlement d'examen PECB ainsi que le règlement de certification PECB.

Modalités d'évaluation

Etude de cas

Pré-requis

Suivre cette formation **Lead Forensics Examiner** ne nécessite aucun prérequis.

Public

Cette formation s'adresse aux publics suivants :

- spécialistes et consultants en informatique judiciaire ;
- professionnels de la cybersécurité ;
- analystes en cyber intelligence ;
- analystes de données électroniques ;
- spécialistes impliqués dans la récupération des preuves informatiques ;
- professionnels souhaitant comprendre l'application de la loi dans le domaine ;
- professionnels souhaitant renforcer leurs savoirs en analyse des investigations informatiques ;
- professionnels et conseillers impliqués dans la sécurité et les technologies de l'information ;
- responsables de l'examen des médias impliqués dans l'extraction et la divulgation de données.

Cette formation s'adresse aux profils suivants

Responsable Sécurité / RSSI
Responsable informatique
Directeur des Systèmes d'Information (DSI)

Analyste risques

Programme

Jour 1 : Introduction à l'investigation informatique et la gestion des incidents

- la norme ISO 27037:2012.
- les approches scientifiques et juridiques de l'informatique judiciaire ;
- les fondamentaux de la réponse aux incidents et des opérations judiciaires informatiques ;
- les pratiques promues par le DoJ et le NIST ;
- les exigences du laboratoire d'investigation informatique.

Jour 2 : Préparation et encadrement d'une enquête informatique judiciaire

- l'enquête numérique ;
- enquêter sur la criminalité informatique ;
- les systèmes d'exploitation et systèmes de fichiers communs ;
- les appareils mobiles ;
- maintenir la chaîne des preuves : politiques et procédures ;

Jour 3 : Analyser et gérer les artefacts numériques

- outils libres et outils commerciaux ;
- les artefacts numériques : identification, acquisition, analyse et communication ;
- utiliser les outils d'investigation informatique et les outils libres ;
- simuler des incidents numériques.

Jour 4 & 5 : Etude de cas et jeux de simulation

- comprendre les menaces émergentes ;
- présentation des résultats numériques judiciaires ;
- présentation des preuves devant une cour de justice.

Dernière demi-journée

- passage de l'examen **PECB Lead Computer Forensics Examiner** (durée 3 heures).

Contenu de formation proposé par PECB