Lead Forensics Examiner : enquêteur judiciaire en criminalistique numérique

Date et durée

Code formation : CLFE
Durée : 4,5 jours
Nombre d'heures : 31 heures

Formation avec certification

PECB Certified Lead Forensics Examiner

Description

La **criminalistique numérique** ou l'investigation informatique légale est un ensemble de méthodes et de techniques visant à identifier et collecter des preuves numériques sur un réseau ou un appareil informatique à la demande d'une instance judiciaire. Le **Lead Forensics Examiner** est la personne en charge de mener ou de superviser l'ensemble des procédures d'investigation au sein d'un réseau informatique d'une entreprise ou d'une organisation.
La **formation Lead Forensics Examiner** vous apprendra à comprendre et à maîtriser les activités de criminalistique numérique dans un cadre judiciaire avec les meilleures pratiques liées à l'exploitation et à la protection des preuves. Vous comprendrez en outre **les bases de l'informatique légale**, la mise en œuvre des processus de récupération de preuves et les techniques d'analyse. Ce programme est axé sur les compétences essentielles requises pour collecter et analyser des datas à partir de système d'exploitations comme Windows, MAC OS X, Linux ou encore Android et IOS.
Après avoir terminé ce programme de formation, vous serez prêt à passer l'examen Lead Forensics Examiner. Celui-ci vous permettra d'obtenir l'un des 3 titres du PECB tels que le **Certified Provisional Forensics Examiner** , qui ne nécessite aucune expérience professionnelle. En décrochant une certification, vous prouverez que vous avez les compétences suffisantes pour réaliser des analyses forensiques, **rédiger des rapports et collecter des preuves** nécessaires à la bonne conduite d'enquêtes forensiques avancées.
Télécharger le guide de formation PECB 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 PECB Certified Lead Computer Forensics Examiner et obtenir une certification.

Cette formation présente aussi de **nombreux avantages applicables** aux organisations de toute taille dans le domaine de la sécurité informatique 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.

Points forts

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

Après avoir réussi cet **examen de 3 heures** vous pourrez demander l'une des certifications suivantes en fonction de votre expérience professionnelle :

Qualification	Expérience professionnelle	Expérience en informatique légale	Autres exigences
PECB Certified Provisional Forensics Examiner	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified Forensics Examiner	2 ans dont 1 an d'expérience dans le domaine de la cybersécurité	Activités de projet totalisant 200 heures	Signer le Code de déontologie de PECB
PECB Certified Lead Forensics Examiner	5 ans dont 2 ans d'expérience dans le domaine de la cybersécurité	Activités de projet totalisant 300 heures	Signer le Code de déontologie de PECB

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

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Suivre la **formation Lead Forensics Examiner** nécessite le prérequis suivant :

- une bonne connaissance en matière de criminalistique informatique est fortement conseillée.

Public

Cette formation s'adresse aux publics suivants :

- les spécialistes et consultants en informatique légale ;
- les experts en cybersécurité qui souhaitent renforcer leurs connaissances en matière de criminalistique informatique ;
- les analystes du cyber renseignement ;
- les spécialistes de la récupération de preuve numérique ;
- tous les professionnels informatique souhaitant comprendre comment se déroule le processus judiciaire dans le domaine de la cybercriminalité ;
- les professionnels et consultants impliqués dans la sécurité et les technologies de l'information ;
- les critiques médias impliqués dans l'extraction et la divulgation de données.

Cette formation s'adresse aux profils suivants

Directeur des Systèmes d'Information (DSI)
Analyste cybersécurité
Administrateur réseaux - télécoms
Chef de projet / Responsable de projet

Programme

Jour 1 : introduction à l'investigation informatique et à 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

- Qu'est qu'une enquête numérique légal ?
- Les processus d'enquête sur la criminalité informatique.
- Les systèmes d'exploitation et les systèmes de fichiers communs.
- Les appareils mobiles.
- Le maintien de la chaîne des preuves : politiques et procédures.

Jour 3 : Analyser et gérer les artefacts numériques

- Les outils libres et les outils commerciaux ;
- Les artefacts numériques : identification, acquisition, analyse et communication.
- Les bonnes pratiques d'utilisation des outils d'investigation informatique.
- Les étapes de simulation des incidents numériques.

Jour 4 & 5 : mise en œuvre d'une étude de cas et des 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 de certification Lead Computer Forensics Examiner (durée 3 heures).

A savoir : ***le support du cours PECB Lead Computer Forensics Examiner est disponible uniquement en anglais.***

Contenu de formation proposé en partenariat avec PECB