Formation Lead Forensics Examiner + Certification

Présentation

- Spécialistes en informatique judiciaire
- Consultants en informatique judiciaire
- Professionnels de cybersécurité
- Analystes de Cyber intelligence
- Analystes de données électroniques
- Spécialistes en récupération des preuves informatiques
- Professionnels qui travaillent ou qui s'intéressent à l'application de la loi
- Professionnels souhaitant approfondir leurs connaissances en analyse des investigations informatiques
- Membres de l'équipe chargée de la sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Personnes responsables de l'examen des médias pour en extraire et divulguer des données
- Spécialistes des TI

Durée : 35,00 heures (5 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre les rôles et les responsabilités d'un Lead Computer Forensics Examiner au cours de l'enquête judiciaire informatique
- Comprendre le but de l'examen des médias électroniques et sa relation avec les normes et méthodologies communes
- Comprendre la séquence correcte des étapes d'une enquête sur un incident informatique et d'une opération d'investigation légale numérique
- Comprendre les outils communs et les outils libres qui peuvent être utilisés lors d'une enquête d'incident et d'une opération judiciaire numérique
- Acquérir les compétences nécessaires pour planifier et exécuter une opération informatique judiciaire, mettre en œuvre et maintenir un réseau de sécurité pour protéger les preuves

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Prérequis

Les connaissances en informatique judiciaire sont recommandées.

Public

En partenariat avec PECB, La formation Lead Computer Forensics Examiner vous permettra d'acquérir l'expertise nécessaire pour exécuter les processus relatifs à l'investigation judicaire afin d'obtenir des preuves numériques complètes et fiables.

Durant de cette formation, vous obtiendrez également une compréhension approfondie des fondamentaux de l'informatique légale, basée sur les bonnes pratiques utilisées pour mettre en œuvre le processus de récupération des preuves forensiques et des techniques analytiques.

Programme de la formation

J1 : Introduction à la réponse aux incidents et concepts relatifs à l'investigation informatique

- Explorer l'ISO 27037
- Principes scientifiques et juridiques relatifs à l'informatique judicaire
- Principes fondamentaux de la réponse aux incidents et des opérations judiciaires informatiques
- Exploration des meilleures pratiques mentionnées dans diverses lignes directrices du DoJ et des lignes directrices NIST
- Exigences relatives au laboratoire d'investigation informatique

J2 : Préparer et diriger une enquête informatique judiciaire

- Enquête sur la criminalité informatique et l'enquête numérique
- Systèmes d'exploitation et systèmes de fichiers communs
- Appareils mobiles
- Maintien de la chaîne des preuves
- Politiques et procédures pour maintenir la chaîne des preuves

J3 : Analyse et gestion des artefacts numériques

- Introduction aux outils libres et aux outils commerciaux
- Identifier, acquérir, analyser et communiquer des artefacts numériques

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Utilisation d'outils d'investigation informatique et d'outils libres
- Simulation d'incident

J4 : Présentation du cas et jeux de simulation

- Les menaces émergentes
- Présenter des résultats numériques judiciaires
- Présenter les preuves devant une cour de justice

J5 : Examen de certification

- Synthèse des acquis, conseils pratiques

Cette formation vous prépare à l'examen de certification de PECB. (Certification incluse)

- Langue : Anglais
- Durée : 3 heures
- Format : Examen en ligne

L'examen couvre les domaines de compétences suivants :

- **Domaine 1** : Principes et concepts fondamentaux de l'investigation informatique
- **Domaine 2** : Meilleures pratiques en investigation informatique
- **Domaine 3** : Exigences relatives au laboratoire légal numérique
- **Domaine 4** : Système d'exploitation et structure de système de fichiers
- **Domaine 5** : Appareils mobiles
- **Domaine 6** : Enquête sur la criminalité informatique et examen forensique
- **Domaine 7** : Maintien de la chaîne des preuves

Pour de plus amples informations concernant l'examen, veuillez consulter Politiques et règlement d'examen.
En cas d'échec, les candidats ont l'opportunité de présenter à nouveau l'examen dans un délai de 12 mois après leur première tentative.

Organisation

Formateur

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France