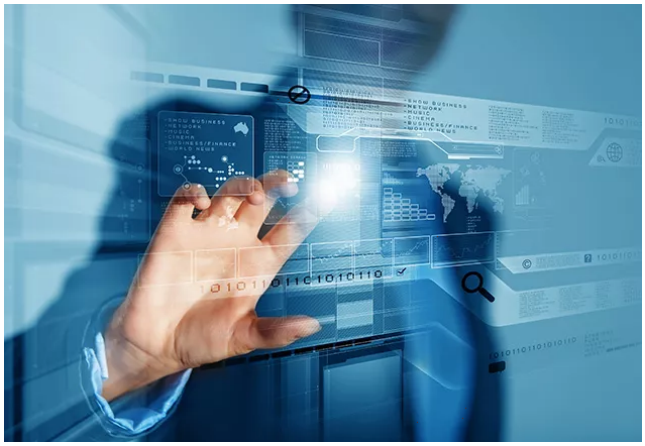
Lead Forensic Examiner

Ref: PR-CYB-CD-LFE

Maîtrisez les concepts et outils d’analyses forensiques dans un contexte judiciaire, ainsi que dans un contexte d’entreprise



DURÉE : **5 Jours** (35H)
Prix : **3 590,00 € HT**

PRÉSENTIEL
FORMATION QUALIFIANTE

Objectifs et compétences visés

- 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.

À qui s'adresse la formation ?

Profils

Analyste sécurité. Analyste SOC. Membre d’une équipe de réponse à incident. Auditeur en test d’intrusion. Responsables des systèmes d’information ou de la sécurité du SI. Toute personne souhaitant maîtriser les principes techniques d’une

analyse forensique.

Prérequis

Aucun prérequis n'est nécessaire à cette formation. Il est nécessaire de venir muni d'un ordinateur portable.

Contenu de la formation

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.

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.

Analyse et gestion des artefacts numériques

- Introduction aux outils libres et aux outils commerciaux.
- Identifier, acquérir, analyser et communiquer des artefacts numériques.
- Utilisation d'outils d’investigation informatique et d'outils libres.

Présentation du cas et jeux de simulation

- Les menaces émergentes.
- Présenter des résultats numériques judiciaires.

- Présenter les preuves devant une cour de justice.

Révisions et examen de certification

Modalités

Modalités d'évaluation

Passage d'un examen de certification PECB.

Nos plus

- Formation animée par un consultant CNPP certifié Lead Forensic Examiner et expert en investigation numérique.
- Disponible en visioconférence.

En bref

21000
stagiaires / an

Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

+33 (0)8 06 00 03 80