EduGroupe
Accompagner pour réussir

Certified Lead Forensics Examiner

Référence : **SECCLFE** Durée : **5 jours (35 heures)** Certification : **PECB**

Connaissances préalables

- Connaissance du système Linux/windows/mobile
- Connaissance réseaux et modèle OSI
- Les principes de réponse à Incident

Profil des stagiaires

- Analyste de données
- Analyste de media électronique
- Consultant
- Membre d'équipe sécurité
- Spécialiste en recherche et récupération de preuves informatiques
- Spécialiste investigation informatique

Objectifs

- Comprendre les concepts et référentiels du forensique
- Appréhender une analyse sur les environnements Linux/Windows/mobile.
- Connaissance des outils et source de veille

Certification préparée

PECB Certified Lead Computer Forensics Examiner. Pour connaître tous les détails concernant les prérequis relatifs au passage de l'examen de certification en ligne, nous vous invitons à cliquer ici pour accéder à la documentation officielle du certificateur

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Inforensique

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Présentation et méthodologie

- Objectifs et structure du cours
- Introduction aux Forensiques
- Méthodologie et référentiel de l'inforensique
- Processus et gestion des incidents
- Les preuves et leurs traitements
- Processus d'analyse & préparation de l'analyse
- Réponse initiale – La trousse à outils

2. Réponse initiale et acquisition des preuves

- Réponse initiale – Préparation et analyse : Linux Collecte informations, memdump - Windows Collecte Information, memdump - Mobile (Android, iOS)
- Présentation des systèmes de fichiers
- Duplication – Précautions et Méthodologie
- Duplications d'images de disque

3. Montage des disques et analyses

- Préparation à l'analyse du système de fichiers
- Analyse des données du système de fichiers – Windows
- Analyse des données du système de fichiers – UNIX/Linux
- Analyse des données du système de fichiers – Mobilité
- Analyse : Le cas du Cloud
- Analyse des emails
- Analyse du web

4. Analyse Réseau

- Rappel OSI
- Utilisation de Wireshark
- Les outils dans wireshark
- Analyse de flux malveillant
- Création de profil forensic

5. Document et Reporting

-

6. Certification PECB Certified Lead Computer Forensics Examiner

- Révision des concepts en vue de la certification
- Examen blanc
- Passage de l'examen écrit de certification en français qui consiste à répondre à 12 questions en 3 heures

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.