EduGroupe
Accompagner pour réussir

Sécurité : Analyse inforensique avancée et réponse aux incidents

Référence : **SECAIARI** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances Linux
- Connaissances Windows

Profil des stagiaires

- Professionnels IT en charge de la sécurité des systèmes d'information, l'investigation légale et la gestion d'incidents

Objectifs

- Être capable de définir et mettre en place un processus de réponse à incident rigoureux
- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires

Certification préparée

- Aucune

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

- 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. JOUR 1

-

2. Mise en place de la réponse à incident

- Préparation à la réponse à incident
- Détection et analyse
- Classification et classement par ordre de priorité
- Notification
- Confinement
- Investigation inforensique
- Eradication et reprise d'activité
- Procédure post-incident
- Que dis la norme ISO 27035

3. Les systèmes de fichiers

- Systèmes de fichiers Windows
- Systèmes de fichiers Linux/BSD

4. L'analyse inforensique et la législation Française

-

5. JOUR 2

-

6. Mise en place d'une analyse inforensique

- Collecte de données et duplication
- Retrouver des fichiers et des partitions supprimés
- Récupération et analyse d'un extraite de mémoire vive
- Analyse des fichiers de logs et corrélation d'événements
- Analyse d'attaques réseaux
- Analyse inforensique des navigateurs
- Analyse inforensique des e-mails

7. JOUR 3

-

8. Mise en place d'une analyse inforensique sur un cas concret

-

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.