Sécurité : Analyse inforensique avancée et réponse aux incidents

Référence : **SECAIARI** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 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 PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Inforensique

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

JOUR 1

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

Les systèmes de fichiers

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

L'analyse inforensique et la législation Française

JOUR 2

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

JOUR 3

Mise en place d’une analyse inforensique sur un cas concret