Analyse Forensique

Lien : https://innov-systems.com/formation/analyse-forensique

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC258

CATÉGORIE
Analyse Apres Incident : Analyse Forensique, Investigation Numérique et Plan de Continuité

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Acquérir les qualifications nécessaires pour réaliser une analyse post-mortem d'incidents de sécurité informatique

POUR QUI ?

- Administrateurs système ou réseau
- Responsables sécurité

Programme détaillé

1 / Introduction

- Définition du Forensic
- Les types de Forensics
- Périmètre de l’investigation
- Trousse à outil
- Méthodologie « First Responder »
- Analyse Post-mortem

2 / La cybercriminalité moderne

- Types de criminalité
- Cadre de gestion d'un incident de sécurité
- Analyser et comprendre les attaques réseaux
- Détection réseau d'intrusions
- Outils de protection

3 / La preuve numérique

- Définition, rôle, types et règles de classement
- Evaluer et sécuriser les éléments électroniques d'une scène de crime
- Collecter et préserver l'intégrité des preuves électroniques

4 / Inforensique Windows

- Acquisition, analyse et réponse
- Compréhension des processus de démarrage
- Disques durs
- Introduction aux systèmes de fichiers

Innov Systems

- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows
- Utilisateurs
- Systèmes
- Analyse des journaux
- Analyse du cache, cookie et historique de navigation, historique des événements

5 / Inforensique Linux

- Les bases de l’inforensique sur un poste de travail Linux »
- Les bases de l’inforensique sur un serveur Linux
- Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d’une frise chronologique du système de fichier

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Innov Systems

Prochaines dates programmées

23 au 26 Fév. 2027	Présentiel - Casablanca
20 au 23 Avr. 2027	Présentiel - Casablanca
15 au 18 Juin 2027	Présentiel - Casablanca
10 au 13 Août 2027	Présentiel - Casablanca
05 au 08 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés

Innov Systems