Analyse Forensic : maîtrisez l’investigation numérique et la collecte de preuves cyber

Lien : https://innov-systems.com/formation/analyse-forensic-maitrisez-linvestigation-numerique-et-la-collecte-de-preuves-cyber

DURÉE
5 jours (35h)

RÉFÉRENCE
SI03

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 :

- Comprendre les principes fondamentaux de la forensic numérique
- Maîtriser la méthodologie d’investigation informatique
- Savoir collecter et préserver les preuves numériques
- Analyser des systèmes compromis et des traces d’intrusion
- Exploiter les outils d’analyse forensic
- Identifier les activités malveillantes sur un système
- Réaliser des analyses réseau et malware
- Rédiger des rapports d’investigation clairs et exploitables
- Respecter le cadre légal de la preuve numérique
- Développer une expertise en réponse à incident cyber

POUR QUI ?

- Analystes cybersécurité
- Ingénieurs sécurité informatique
- Experts forensic et investigation numérique
- Administrateurs systèmes et réseaux
- Membres de SOC (Security Operations Center)
- Forces de l’ordre et enquêteurs numériques
- Toute personne impliquée dans la gestion des incidents de sécurité informatique

Innov Systems

Programme détaillé

1 / Introduction à l’analyse forensic

- Définition et enjeux de la forensic numérique
- Rôle dans la cybersécurité et la justice numérique
- Types de forensic (système, réseau, mobile)

2 / Cadre légal et chaîne de conservation des preuves

- Notions juridiques de la preuve numérique
- Chaîne de custody (chaîne de conservation)
- Respect de la conformité et de l’intégrité des données

3 / Méthodologie d’investigation forensic

- Étapes d’une investigation numérique
- Identification, collecte, analyse et reporting
- Approche structurée des incidents

4 / Acquisition des preuves numériques

- Capture des disques et mémoires
- Imagerie forensique bit à bit
- Outils de collecte sécurisée

5 / Analyse des systèmes compromis

- Analyse des systèmes Windows et Linux
- Identification des traces d’intrusion
- Analyse des logs systèmes

Innov Systems

6 / Analyse réseau forensic

- Capture et analyse du trafic réseau
- Détection des communications suspectes
- Analyse des attaques réseau

7 / Analyse des malwares

- Reverse engineering basique
- Comportement des logiciels malveillants
- Identification des signatures d’attaque

8 / Outils d’analyse forensic

- Autopsy, FTK, Volatility
- Wireshark et outils réseau
- Environnements de laboratoire forensic

9 / Rédaction de rapports d’investigation

- Structuration des rapports forensic
- Présentation des preuves techniques
- Vulgarisation pour non-techniciens

10 / Études de cas et simulations d’incidents

- Analyse d’attaques réelles
- Scénarios de compromission
- Exercices pratiques d’investigation

Innov Systems

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

Prochaines dates programmées

07 au 11 Déc. 2026	Présentiel - Casablanca
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca

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

Innov Systems

Réservation & Renseignements

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

Innov Systems — Tous droits réservés