



Analyse Forensique et Réponse à Incidents de Sécurité

Lien : <https://innov-maroc.com/formation/analyse-forensique-et-reponse-a-incidents-de-securite>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
SEC259

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

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
- ✓ Maîtriser le processus de réponse à incident

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 / Collecte des informations

- Hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Security Event Information Management (SIEM), événements collectés du SI
- Journaux système des équipements (firewalls, routeurs, serveurs, bases de données)

4 / Examen des journaux (logs)

- Visualiser, trier, chercher dans les traces
- Comprendre les attaques : Splunk

5 / 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

6 / Infoforensique Windows

- Acquisition, analyse et réponse
- Compréhension des processus de démarrage
- Disques durs
- Introduction aux systèmes de fichiers
- 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 logs
- Analyse du cache, cookie et historique de navigation, historique des événements

7 / Infoforensique Linux

- Les bases de l'infoforensique sur un poste de travail Linux »
- Les bases de l'infoforensique sur un serveur Linux

- Logs 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

Prochaines dates programmées

 26 au 30 Oct. 2026

 Distanciel

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

Réservation & Renseignements

 **Téléphone** : +212 522 247 210

 **Email** : contact@innov-maroc.com

 **Web** : <https://www.innov-maroc.com>

Document généré le 12/10/2026 — Réf : SEC259

INNOV MAROC — Tous droits réservés