Forensics Windows : maîtrisez l’investigation numérique et l’analyse des preuves digitales

Lien : https://innov-systems.com/formation/forensics-windows-maitrisez-linvestigation-numerique-et-lanalyse-des-preuves-digitales

DURÉE
5 jours (35h)

RÉFÉRENCE
SI18

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 de la forensic numérique sur Windows
- Savoir collecter et préserver des preuves numériques
- Analyser le système de fichiers et le registre Windows
- Exploiter les journaux système pour l’investigation
- Réaliser une analyse mémoire (RAM forensic)
- Identifier des activités suspectes ou malveillantes
- Utiliser les outils professionnels de forensic Windows
- Appliquer une méthodologie rigoureuse d’investigation
- Rédiger des rapports d’analyse forensique structurés
- Développer des compétences en cybersécurité et investigation numérique

POUR QUI ?

- Analystes en cybersécurité
- Experts en forensic numérique
- Administrateurs systèmes Windows
- Forces de l’ordre et enquêteurs numériques
- Ingénieurs sécurité IT
- Responsables SOC (Security Operations Center)
- Toute personne impliquée dans l’investigation numérique sur environnements Windows

Innov Systems

Programme détaillé

1 / Introduction au forensic numérique sur Windows

- Définition de la digital forensics
- Rôle de l’investigation sur systèmes Windows
- Cadre légal et chaîne de conservation des preuves

2 / Architecture des systèmes Windows

- Fonctionnement du système de fichiers NTFS
- Registre Windows et journaux système
- Gestion des utilisateurs et permissions

3 / Méthodologie d’investigation forensique

- Processus d’acquisition des preuves
- Préservation de l’intégrité des données
- Documentation de la scène numérique

4 / Collecte des preuves numériques

- Imagerie disque et mémoire vive
- Extraction des fichiers système
- Collecte des logs et artefacts

5 / Analyse du système de fichiers

- Analyse NTFS et métadonnées
- Récupération de fichiers supprimés
- Analyse des timelines système

Innov Systems

6 / Analyse des journaux Windows

- Event Viewer et logs système
- Détection d’activités suspectes
- Corrélation des événements

7 / Analyse des artefacts utilisateurs

- Historique de navigation
- Fichiers récents et traces d’activité
- Analyse des périphériques connectés

8 / Analyse mémoire (RAM Forensics)

- Extraction de la mémoire vive
- Analyse des processus actifs
- Détection de malware en mémoire

9 / Outils de forensic Windows

- FTK Imager et Autopsy
- Volatility Framework
- Outils de récupération et analyse

10 / Rédaction de rapports d’investigation

- Structuration des rapports forensiques
- Présentation des preuves
- Conclusions et recommandations techniques

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

25 au 29 Jan. 2027	Présentiel - Casablanca
22 au 26 Mars 2027	Présentiel - Casablanca
17 au 21 Mai 2027	Présentiel - Casablanca
12 au 16 Juil. 2027	Présentiel - Casablanca
06 au 10 Sep. 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