Forensics numérique Windows & Linux : investigation post-incident et chaîne de preuve

Lien : https://innov-systems.com/formation/forensics-numerique-windows-linux-investigation-post-incident-et-chaine-de-preuve

DURÉE
5 jours (35h)

RÉFÉRENCE
SI97

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 du forensic numérique Windows et Linux
- Maîtriser la chaîne de conservation des preuves numériques
- Collecter et analyser des artefacts systèmes de manière fiable
- Réaliser des investigations post-incident structurées
- Analyser les logs et traces des systèmes compromis
- Effectuer des analyses mémoire et disque avancées
- Identifier les vecteurs d’attaque et comportements malveillants
- Reconstituer la chronologie d’un incident de sécurité
- Rédiger des rapports d’investigation exploitables juridiquement
- Utiliser les outils de forensic standards du marché
- Améliorer la réponse aux incidents de cybersécurité
- Étudier des cas réels d’attaques et compromissions

POUR QUI ?

- Analystes SOC
- Ingénieurs cybersécurité
- Experts forensic / investigateurs numériques
- Pentesters et Red Teamers
- Administrateurs systèmes Windows et Linux
- Responsables sécurité (RSSI)
- Consultants en cybersécurité
- Ingénieurs réponse à incident (IR/DFIR)
- Forces de l’ordre et enquêteurs cyber
- Auditeurs IT sécurité
- Ingénieurs DevSecOps
- Toute personne impliquée dans la gestion des incidents de cybersécurité et l’investigation numérique

Innov Systems

Programme détaillé

1 / Introduction au forensic numérique

- Définition et rôle de la cyber-investigation
- Types d’incidents et périmètre d’analyse
- Principes fondamentaux de la preuve numérique

2 / Chaîne de conservation des preuves (Chain of Custody)

- Collecte et préservation des artefacts
- Traçabilité et intégrité des preuves
- Cadre juridique et admissibilité en justice

3 / Architecture des systèmes Windows et Linux

- Structures de fichiers (NTFS, ext4)
- Logs systèmes et journaux d’événements
- Points d’analyse critiques

4 / Acquisition des données forensic

- Imagerie disque et mémoire RAM
- Outils de collecte (FTK Imager, dd, Velociraptor)
- Précautions anti-altération

5 / Analyse des artefacts Windows

- Registre Windows et traces système
- Event Logs et journaux de sécurité
- Historique utilisateur et artefacts persistants

Innov Systems

6 / Analyse des artefacts Linux

- Logs système (/var/log)
- Shell history et cron jobs
- Processus, connexions réseau et traces système

7 / Analyse mémoire (Memory Forensics)

- Dump mémoire et analyse volatile
- Détection de malware en mémoire
- Outils (Volatility, Rekall)

8 / Investigation des malwares et intrusions

- Analyse de comportements suspects
- Reverse engineering basique
- Corrélation des indicateurs de compromission (IOC)

9 / Corrélation et reconstruction des événements

- Timeline des attaques
- Corrélation multi-sources
- Identification du vecteur initial d’intrusion

10 / Reporting et remédiation post-incident

- Rédaction de rapports forensic
- Recommandations de sécurité
- Amélioration de la posture de défense

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

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 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