Analyse Forensique des Systèmes Windows et Linux

Lien : https://innov-systems.com/formation/analyse-forensique-des-systemes-windows-et-linux

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC291

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 et maîtriser le processus complet d’investigation numérique sur environnements Windows et Linux
- Savoir identifier, acquérir et analyser les données critiques issues de supports numériques
- Exploiter efficacement les artefacts système et traces numériques pour reconstruire les événements
- Maîtriser les outils et techniques de réponse à incident et d’analyse post-mortem
- Savoir corréler les journaux systèmes, réseaux et applicatifs pour identifier les causes d’incidents
- Développer une méthodologie rigoureuse et conforme aux bonnes pratiques d’investigation numérique

POUR QUI ?

- Administrateurs et ingénieurs systèmes et réseaux
- Responsables sécurité (RSSI, SOC analystes)
- Enquêteurs numériques et experts techniques en réponse à incident
- Professionnels de la cybersécurité souhaitant se spécialiser en analyse forensique

Programme détaillé

1 / FONDEMENTS DE L'ANALYSE FORENSIQUE

- Définitions, enjeux et typologie des investigations numériques
- Rôles, responsabilités et cadre légal de l'investigateur
- Les grands principes de la chaîne de possession des preuves
- Typologie des environnements : postes, serveurs, environnements virtualisés

2 / MÉTHODOLOGIE D'INVESTIGATION ET RÉPONSE À INCIDENT

- Phases du processus forensique : identification, acquisition, préservation, analyse, rapport
- Méthodologie « First Responder » et gestion des scènes numériques
- Préparation et planification d'une réponse à incident

3 / OUTILLAGE ET ENVIRONNEMENT DE TRAVAIL

- Panorama des outils forensiques : FTK Imager, Autopsy, Magnet AXIOM, Volatility, X-Ways
- Construction d'un laboratoire forensique virtuel
- Bonnes pratiques de manipulation et de stockage des images disques

4 / SYSTÈMES DE FICHIERS ET STRUCTURES INTERNES

- Introduction aux systèmes de fichiers : NTFS, FAT, exFAT
- Lecture et interprétation des métadonnées
- Horodatages et cohérence temporelle

5 / ACQUISITION DES DONNÉES : VOLATILES ET PERSISTANTES

- Techniques d'acquisition à chaud et à froid
- Gestion des supports chiffrés et des disques virtuels
- Extraction des données de la RAM et hyberfiles.sys

Inov Systems

- Vérification et intégrité des acquisitions

6 / ANALYSE DES ARTEFACTS WINDOWS

- Registres Windows : clés systèmes et utilisateurs
- Historique d’exécution, ouverture de fichiers, périphériques USB
- Analyse des journaux d’événements : sécurité, système, application
- Extraction des artefacts de navigation (Edge, Chrome, Firefox)

7 / RECHERCHE DE DONNÉES SUPPRIMÉES ET ESPACES NON ALLOUÉS

- Concepts de carving et reconstruction de fichiers
- Exploitation des Volume Shadow Copies et sauvegardes automatiques
- Gestion des aléas du stockage SSD/Flash

8 / CORRÉLATION ET RECONSTITUTION DES ÉVÉNEMENTS

- Création de frises chronologiques d’événements
- Corrélation entre journaux Windows, navigateurs et applications
- Analyse de scénarios : exécution de logiciels malveillants, exfiltration de données

9 / ANALYSE DES COMMUNICATIONS ET INTERACTIONS INTERNET

- Analyse des journaux SMTP, clients de messagerie et logs serveurs
- Traces web : cookies, cache, historique et téléchargements
- Exploitation des données EXIF et géolocalisation

10 / BASES DE L’ANALYSE FORENSIQUE LINUX

- Structure du système de fichiers Linux : ext4, journaux systèmes
- Analyse des artefacts d’activité : bash history, syslog, auth.log
- Analyse de la mémoire et processus actifs

Inov Systems

11 / INVESTIGATION SUR SERVEUR WEB

- Identification des artefacts serveurs : Apache, Nginx, PHP logs
- Corrélation entre journaux applicatifs et traces réseau
- Reconstruction d’incidents d’intrusion web
- Cas pratique : compromission d’un serveur Linux hébergeant un site

12 / ATELIER COMPLET D’INVESTIGATION NUMÉRIQUE

- Analyse d’un cas d’incident : fuite d’informations sensibles
- Acquisition, tri et extraction des données pertinentes
- Corrélation et interprétation des événements
- Présentation d’un rapport d’investigation conforme aux standards (ENFSI, ISO/IEC 27037)

13 / BONNES PRATIQUES ET OUTILS D’OPTIMISATION

- Automatisation avec PowerShell et Python
- Interrogation de gros volumes de données (Elastic, Timesketch)
- Construction d’une base de connaissances d’artefacts

14 / SYNTHÈSE ET ÉVALUATION

- Quiz d’évaluation des acquis
- Débriefing collectif : erreurs fréquentes et retours d’expérience
- Recommandations pour la certification en forensic numérique

Inov 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

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 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