Préparation à la certification GCFA

Non-certifiante | Formation continue

Réf. : 25190248F — Mise à jour : 1 décembre 2025

Organisme responsable : **IT MANAGEMENT INSTITUTE**

Présentation de la formation

Objectifs

- **Identifier les concepts clés liés à l'analyse forensique avancée, à la réponse à incident et à l'investigation des systèmes d'exploitation (Windows, Linux),** afin de disposer d'une base théorique solide pour la mise en pratique et la préparation à l'examen GCFA.
- **Mettre en œuvre les outils et méthodes présentés en formation** pour la collecte, l'analyse et la corrélation d'artefacts avancés (registre, journaux, mémoire, systèmes de fichiers) dans des situations professionnelles concrètes de compromission.
- **Évaluer les résultats obtenus et élaborer des rapports d'investigation clairs,** pour développer une capacité d'analyse et d'adaptation conforme aux attentes de la certification GCFA.

Programme

Module 1 : Rappel des fondamentaux et préparation à l'examen GCFA

- Structure et méthodologie de l'examen GCFA
- Stratégies de révision et gestion du temps
- Rappel des chaînes de conservation et des aspects légaux

Module 2 : Forensique Avancée Windows

- Analyse détaillée du Registre Windows pour la persistance et l'exécution
- Investigation des artefacts d'utilisation (ShellBags, JumpLists, AppCompatCache, SRUM)
- Analyse approfondie des journaux d'événements (Event Logs) et de l'historique
- Introduction à l'analyse de la mémoire vive (Memory Forensics) sur Windows

Module 3 : Forensique Linux et macOS

- Artefacts spécifiques aux systèmes basés sur UNIX (journaux, historique des commandes, structure du système de fichiers)
- Identification des mécanismes de persistance sur Linux/macOS (crontab, services, etc.)
- Outils d'analyse forensique spécifiques à ces environnements

Module 4 : Réponse à Incident et Investigation Réseau

- Processus de réponse à incident et intégration de la forensique
- Corrélation d'événements et construction de la chronologie d'attaque (Timeline)
- Analyse des traces réseau (PCAP) liées à l'incident
- Identification des menaces et des techniques de l'attaquant (TTPs)

Certifications préparées et métiers visés

Niveau d'entrée	Niveau de sortie
Sans niveau spécifique	**Sans niveau spécifique**

Métiers associés

M1801 — Administration de systèmes d'information

M1802 — Expertise et support en systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
2140855S	À distance	—	01/12/2025	31/12/2026

Source : GREF Bretagne #25190248F