ANALYSE INFORENSIQUE AVANCÉE ET RÉPONSE AUX INCIDENTS

Préparez-vous à l'analyse post-incident

Code : AIARI

Ce cours vous apprendra à mettre en place une procédure complète d'analyse inforensique sur des environnements hétérogènes.

Vous y aborderez la réponse aux incidents d'un point de vue organisationnel.

Vous étudierez également les méthodologies et outils appropriés utilisés dans la phase technique de la réponse aux incidents, à savoir l'analyse inforensique (ou post-incident).
À l'issue de la formation, vous serez capable de préserver les preuves numériques pour en effectuer l'analyse ultérieure et les présenter dans le cadre d'un recours judiciaire.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Les bases de la réponse aux incidents et de l'analyse inforensique

- Mise en place de la réponse aux incidents
  - Préparation à la réponse aux incidents
  - Détection et analyse
  - Classification et classement par ordre de priorité
  - Notification
  - Confinement
  - Investigation inforensique
  - Éradication et reprise d'activité
- Outils et équipements de surveillance
- Méthodologie et outillage pour l'analyse inforensique
  - S'organiser
  - Choisir ses outils
  - Respecter les méthodes scientifiques
  - Présenter ses conclusions dans un rapport

JOUR 2

Approche de l'analyse inforensique sur les principaux domaines techniques

- Collecte de données et duplication
  - Comprendre les systèmes de fichiers Windows, Linux et BSD
  - Outils et moyens de collecte
- Retrouver des partitions et des fichiers supprimés
- Analyse de journaux d'évènements des différents équipements
- Analyse d'attaques réseaux
  - Les sources de capture
  - Revue d'attaques répandues

JOUR 3

Analyses ciblées et exercices avancés

- Analyse des fichiers de journaux et corrélation d'événements
  - Utiliser un indexeur (ELK)
- Analyse inforensique des navigateurs
- Acquisition et analyse de la mémoire (Volatility)
- Analyse inforensique des e-mails
- Écriture d'un rapport (bonnes pratiques et méthode PRIS)

Mise en pratique sur des cas concrets.

PROCHAINES DATES

20 mars 2024
27 novembre 2024

OBJECTIFS

- Être capable de définir et mettre en place un processus de réponse aux incidents rigoureux
- Collecter correctement les preuves nécessaires à une analyse de qualité et à d'éventuelles poursuites judiciaires
- Donner aux participants les qualifications nécessaires pour identifier et analyser les traces laissées lors de l'intrusion

INFORMATIONS GÉNÉRALES

Code : AIARI
Durée : 3 jours
Prix : 2 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Professionnels IT en charge de la sécurité des systèmes d'information, de la réponse aux incidents ou de l'investigation légale

PRÉ-REQUIS

- Avoir une bonne culture générale en informatique
- Maîtriser Linux (administration, commandes et programmation shell)
- Avoir des connaissances générales des attaques et vulnérabilités (des rappels pourront être effectués)
- Avoir des connaissances générales en administration Windows

RESSOURCES

- Support de cours
- 60% d'exercices pratiques
- 1 PC par personne
- Environnement Linux et Windows
- Machines virtuelles