Forensics Windows

Cours Pratique de 5 jours - 35h
Réf : FOH - Prix 2024 : 3 530CHF HT

Après une attaque informatique, l'investigation forensic permet de collecter et d'analyser des éléments ayant valeur de preuve en vue d'une procédure judiciaire. L'objectif principal est donc la récupération et l'analyse de données prouvant un délit numérique.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Gérer une investigation numérique sur un ordinateur Windows

Analyser l'intrusion a posteriori

Collecter et préserver l'intégrité des preuves électroniques

TRAVAUX PRATIQUES

Formation alternant théorie et pratique. Tout ce qui est appris sera expérimenté.

LE PROGRAMME

dernière mise à jour : 05/2022

1) Présentation de l'inforensique

- Périmètre de l'investigation.
- Trousse à outil, méthodologie "First Responder" et analyse Post-mortem.
- Disques durs, introduction aux systèmes de fichiers et horodatages.
- Acquisition des données (persistantes et volatiles) et gestion des supports chiffrés.
- Recherche de données supprimées.
- Sauvegardes, Volume Shadow Copies et aléas du stockage flash.
- Registres Windows et structures de registres.
- Analyse des journaux, évènements / antivirus / autres logiciels.

2) Scénario d'investigation

- Téléchargement / accès à des contenus confidentiels.
- Exécution de programmes, traces de manipulation de fichiers et de dossiers.
- Fichiers supprimés, espace non alloué et carving.
- Géolocalisation et photographies (données Exifs).
- Journaux SMTP : acquisition coté serveur, analyse client messagerie.
- Points d'accès WiFi et périphérique USB.
- HTML5, courriels et utilisateurs abusés par des logiciels malveillants.
- Exfiltration d'informations.

3) Interaction sur Internet

- Office 365.
- Sharepoint.
- Traces sur les AD Windows.
- Présentation des principaux artefacts.
- Bases de l'analyse de la RAM.
- Utilisation des navigateurs Internet.
- Chrome / IE / Edge / Firefox.

PARTICIPANTS

Personnes souhaitant se lancer dans l'inforensique. Administrateurs système Windows. Experts de justice en informatique.

PRÉREQUIS

Avoir de solides bases en sécurité des systèmes d'information.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

4) Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux.
- Les bases de l'inforensique sur un serveur Linux : journaux serveurs Web & corrélations avec le système de fichiers.
- Création et analyse d'une frise chronologique du système de fichier.

5) Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts.
- Exemple d'outils d'interrogation de gros volume de données.

LES DATES

CLASSE À DISTANCE
2024 : 01 juil., 07 oct., 09 déc.