Analyse Forensic

Cours Pratique de 3 jours - 21h
Réf : AFB - Prix 2024 : 2 390CHF HT

Réaliser une analyse post-mortem (aussi appelée inforensic) d'incidents de sécurité informatique est devenue essentiel pour préserver des preuves. Suite à des simulations d'attaques, vous apprendrez à collecter et préserver les preuves, les analyser et améliorer la sécurité du SI après l'intrusion.

OBJECTIFS PÉDAGOGIQUES

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

Maîtriser les bons réflexes en cas d'intrusion sur une machine

Collecter et préserver l'intégrité des preuves électroniques

Analyser l'intrusion a posteriori

LE PROGRAMME

dernière mise à jour : 07/2022

1) Comment gérer un incident ?

- Les signes d'une intrusion réussie dans un SI.
- Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
- Comment réagir face à une intrusion réussie ?
- Quels serveurs sont concernés ?
- Savoir retrouver le point d'entrée et le combler.
- La boite à outils Unix/Windows pour la recherche des preuves.
- Nettoyage et remise en production des serveurs compromis.

2) Analyser les incidents pour mieux se protéger : L'analyse Forensic

- Informatique judiciaire : types de crimes informatiques, rôle de l'enquêteur informatique.
- La cybercriminalité moderne.
- La preuve numérique.

3) Analyse forensic d'un système d'exploitation Windows

- Acquisition, analyse et réponse.
- Compréhension des processus de démarrage.
- Collecter les données volatiles et non volatiles.
- Fonctionnement du système de mot de passe, du registre Windows.
- Analyse des données contenues dans la mémoire vive, des fichiers Windows.
- Analyse du cache, cookie et historique de navigation, historique des événements.

Travaux pratiques : Injection d'un utilisateur. Casser le mot de passe. Collecter, analyser les données de la mémoire vive. Référencer, faire le hash de tous les fichiers. Explorer les données du navigateur, du registre.

PARTICIPANTS

Ingénieur/administrateur systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en sécurité informatique et en réseaux/systèmes. Avoir suivi le cours "Collecte et analyse des logs, optimiser la sécurité de votre SI".

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.

LES DATES

CLASSE À DISTANCE
2024 : 05 juin, 23 sept., 27 nov.