Analyse Forensic et réponse à incidents de sécurité

Cours Pratique de 4 jours - 28h
Réf : AFR - Prix 2024 : 2 810CHF HT

Ce stage Forensic avancé vous montrera les techniques indispensables pour réaliser une analyse après la survenue d'incidents de sécurité informatique. Au travers de nombreuses simulations, vous apprendrez à collecter, analyser et surtout préserver les preuves, et ainsi améliorer la sécurité du SI.

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

Améliorer sa sécurité après une intrusion

TRAVAUX PRATIQUES

Investigation des traces de tout type, de mémoire de masse, collecte, analyse, amélioration de la sécurité globale (mise en œuvre de contre-mesures).

LE PROGRAMME

dernière mise à jour : 03/2021

1) Analyse forensic (ou inforensic) des systèmes

- Informatique judiciaire. Types de crimes informatiques.
- Rôle de l'enquêteur informatique.

2) Cybercriminalité moderne

- Types de criminalité.
- Cadre de gestion d'un incident de sécurité, CERT.
- Analyser et comprendre les attaques réseaux.
- Détection réseau d'intrusions.
- Outils de protection, législation française.

Travaux pratiques : Analyser des logs réseaux d'un DDoS Volumétrique, ARP. Mise en place de SNORT.

3) Collecte des informations

- Hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Security Event Information Management (SIEM), événements collectés du SI.
- Journaux système des équipements (firewalls, routeurs, serveurs, bases de données).

Travaux pratiques : Géolocalisation d'adresses. Analyse de l'historique des utilisateurs Web (cookie, données envoyées POST). Analyser des logs Web d'une Injection SQL et mise en place de contre-mesure.

4) Analyse de logs

- Visualiser, trier, chercher dans les traces.
- Splunk pour comprendre les attaques.

Travaux pratiques : Installer, configurer Splunk. Analyser des logs Web d'un Brute-Force sur Formulaire, mise en place de contre-mesure.

PARTICIPANTS

Ingénieurs/administrateurs systèmes et réseaux, responsables de la sécurité.

PRÉREQUIS

Bonnes connaissances en sécurité informatique et en réseaux/systèmes.

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.

5) Preuve numérique

- Définition, rôle, types et règles de classement.
- Evaluer et sécuriser les éléments électroniques d'une scène de crime.
- Collecter et préserver l'intégrité des preuves électroniques.

Travaux pratiques : Dupliquer les données bit à bit, vérifier l'intégrité. Récupérer les fichiers supprimés et/ou cachés. Analyse des données numériques.

6) 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.

LES DATES

CLASSE À DISTANCE
2024 : 18 juin, 24 sept., 19 nov.