Programme de formation

Analyse de Malwares - Les fondamentaux

3 jours - 21 heures	Code formation : ADHSYS0712

adhara France

adhara.fr

Objectifs

Développer les compétences nécessaires pour mener un test d'intrusion.

Participants

Tout administrateur systèmes, ingénieur systèmes et réseaux, chef de projets en sécurité.

Prérequis

Disposer de connaissances de base en réseau TCP/IP ainsi que sur Windows et Linux.

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Remarques

Certification

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d'accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d'une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l'adaptation de l'action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d'émargement signée par demi-journée ainsi que l'évaluation des acquis sont adressées avec la facture.

Programme

Introduction

Fonctionnalités des Malwares
APT, vecteurs d'attaque, classification, symptômes, checklist

Programme de formation

Analyse de Malwares - Les fondamentaux

3 jours - 21 heures	Code formation : ADHSYS0712

adhara France

adhara.fr

Techniques d’analyse des Malwares

Dump de la mémoire
Volatility
Format de fichiers
EXE,Pe (En-têtes, section, IAT, EAT, API Windows, API Fonction, Dll)
Entropie
Techniques d’obfuscation : Packers
Techniques D’évasion Vitual Machine
Anti-debugging
Mesures préventives
Mise en place d'un LAB d'analyse

Analyse statique

Analyse d’un fichier PDF
Extraction JavaScript
Analyse d’un fichier PE
Analyse d’un fichier EXE
Yara Rules

Analyse dynamique

Analyse de registre
Analyse de réseau
Analyse de la mémoire

Les bases de l'asm

Instructions courantes
Rétro-ingénierie (Ransomware)