Sécurité défensive

Analyse de Malwares - Les fondamentaux

2 jours (14h00) | ★★★★★ 5/5 | SEC-MALW | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 21/06/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire les différents types de malwares et leurs objectifs
- Identifier comment les malwares se propagent et infectent les systèmes
- Définir les techniques d'analyse statique et dynamique des malwares
- Reconnaître les signes d'une éventuelle infection par des malwares.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir des connaissances de base en Cybersécurité. Etre familié avec les concepts de base des menaces informatiques ainsi qu'avec l'utilisation de systèmes d'exploitation tels que Linux et Windows. Etre à l'aise avec l'utilisation de la ligne de commande pour des tâches basiques et avoir une expérience avec la virtualisation.

Public concerné

Professionnels de la Cybersécurité, admnistrateurs système, analystes de menaces, gestionnaires de sécurité, étudiants et toute personne souhaitant se former aux fondamentaux des malwares.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1 - Matin

Introduction aux malwares et méthodes de propagation

- Introduction aux malwares
  - Types
  - Objectifs
  - Impacts
- Historique des malwares
  - Evolution
  - Importance dans la Cybersécurité
- Méthodes de propagation
  - Vecteurs de propagation et IoC (Indicator of Compromise)

Jour 1 - Après-midi

Introduction aux malwares et méthodes de propagation - Suite

- Distinction entre l'analyse statique et dynamique des malwares
- Outils d'analyse
  - Aperçu des outils courants

Exemple de travaux pratiques (à titre indicatif)

- *Atelier pratique : configuration d'un environnement de laboratoire pour l'analyse*

Jour 2 - Matin

Analyse de malwares et techniques d'analyse

- Analyse format PE :
  - Examen d'éxécutables Windows
- Analyse format PDF :
  - Exploration des fichiers PDF malveillants

Jour 2 - Après-midi

Analyse de malwares et techniques d'analyse - Suite

- Analyse dynamique format exe
- Analyse dynamique format PDF
- Analyse en ligne de malwares

  - Services en ligne pour analyser des échantillons de malwares
- Bilan du cours et réflexion sur l'application des connaissances

Exemple de travaux pratiques (à titre indicatif)

- *Atelier pratique d'analyse : analyse guidée avec des outils appropriés*

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.