Sécurité défensive

Analyse de Malwares - Niveau avancé

3 jours (21h00) | 9 4,6/5 | SEC-MALW2 | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 27/07/2024.

Objectifs de formation

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

- Exploiter les techniques d'analyse statique et dynamique avancée des malwares
- Reconnaître les outils de débogage et de désassemblage, tels qu'Immunity Debbuger, OllyDbg, GDB, IDA Pro...
- Renforcer les compétences en détection et en réaction aux menaces sophistiquées.

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 suivi le cours SEC-MALW "Analyse de Malwares - Les fondamentaux" ou avoir les connaissances équivalentes. Avoir une expérience avec l'analyse de malwares de base et une connaissance des concepts d'assemblage et d'architecture des systèmes.

Public concerné

Professionnels de la Cybersécurité souhaitant approfondir leurs compétences en analyse de malwares et analystes de menaces cherchant à perfectionner leur capacité à analyser des malwares complexes.

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

Bases de l'assemblage, gestion de la mémoire et récapitulatif

- Récapitulatif sur les fondamentaux des malwares
- Introduction à l'assemblage
  - Comprendre le langage d'assemblage et ses concepts de base
- Architecture des systèmes
  - Aperçu des architectures de processeurs courantes
- Gestion de la mémoire
  - Fonctionnement de la pile et du tas

Jour 1 - Après-midi

Bases de l'assemblage, gestion de la mémoire et récapitulatif - Suite

- Analyse de code assemblé
  - Traduction de code machine en langage d'assemblage

Exemple de travaux pratiques (à titre indicatif)

- *Atelier pratique : écriture et débogage d'un shell code en assembleur*

Jour 2 - Matin

Techniques d'analyse statique avancée

- Revue des concepts clés du jour précédent
- Analyse statique approfondie
  - Désassemblage
  - Désobfuscation
  - Analyse du code malveillant

Jour 2 - Après-midi

Techniques d'analyse statique avancée - Suite

- Utilisation d'IDA Pro
  - Exploration de fonctionnalités avancées

Exemple de travaux pratiques (à titre indicatif)

– *Atelier pratique : analyse statique de malwares complexes avec IDA Pro*

Jour 3 - Matin

Techniques d'analyse dynamique avancée

– Analyse dynamique avancée
  – Utilisation d'Immunity Debugger, OllyDbg, GDB...
– Analyse de hooking et d'injection de code
  – Compréhension des méthodes d'interaction avec les processus

Jour 3 - Après-midi

Techniques d'analyse dynamique avancée - Suite

– Détection des techniques d'évasion
  – Repérage des tentatives de détection de contournement
– Bilan du cours et perspectives

Exemple de travaux pratiques (à titre indicatif)

– *Atelier pratique : analyse dynamique de malwares en utilisant différents débogueurs*

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.