

Analyse de Malwares – Niveau avancé

3 jours (21 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 925 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

Objectifs

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 Debugger, OllyDbg, GDB, IDA Pro...
- Renforcer les compétences en détection et en réaction aux menaces sophistiquées.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

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.

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.

Programme

1 Pendant votre formation

Analyse de Malwares – Niveau avancé

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*

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités 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

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 30 novembre 2026 au 2 décembre 2026 (3 jours / 21 heures)

Paris La Défense

Du 30 novembre 2026 au 2 décembre 2026

Paris La Défense

- 30 novembre 2026 9h00 – 16h00
- 1 décembre 2026 9h00 – 16h00
- 2 décembre 2026 9h00 – 16h00