Formation Analyse de malware : Expert

Objectifs de la formation Analyse de Malware expert

Apprendre à détecter et à contrer les malwares est devenu incontournable pour les informaticiens, quelle que soit leur environnement de travail. Cette formation complète sur l'analyse de Malwares vous permettra d'acquérir à la fois les connaissances théoriques et les connaissances pratiques requises pour réaliser la rétro-ingénierie de malwares.

Plus concrètement, à l'issue de ce cursus de 5 jours vous aurez acquis les connaissances et la pratique pour :

- Savoir analyser des malwares utilisés lors d'APT
- Apprendre à développer des obscurcissements
- Savoir analyser un malware en mode noyau

À qui s'adresse cette formation ?

Public :

Cette formation s'adresse aux analystes des CERT, CSIRT, structures possédant une expérience dans l'analyse de malware ayant besoin d'analyser des codes malveillants complexes.

Prérequis :

Pour suivre ce cours dans de bonnes conditions, il vous faut une très bonne connaissance de Windows, savoir-faire du Reverse Engineering, savoir développer en Python ou Ruby, bien

connaître les API Windows et avoir déjà analysé des malwares. La Formation Analyse de malware : Les Fondamentaux constitue les connaissances minimums à maitriser.

Contenu du cours Analyse de Malware expert

Windbg

Analyse d'un malware utilisé lors d'APT

Persistance non documentée
Dissimulation du code
Détection des anomalies
Machines virtuelles

Reverse Engineering avancé

Communications interprocessus
Techniques d'anti-débug et d'anti-Analyse
Packers et obfuscation avancée
Implémentation de CPU exotique

Automatisation

Désobfuscation
Unpacking

Noyau

Processus de boot
Infection du processus de boot
Modifications de l'espace noyau
PatchGuard
Identification de la présence de rootkit
Emulation du code exécutable
Analyse de deux bootkits 64b

Travaux Pratiques

Résolument tourné vers la sécurité et animé par un expert reconnu, ce cours permettra aux stagiaires de développer des bases solides théoriques et pratiques de l'analyse de malware. Des cas réels de malwares seront utilisés lors de cette formation. Les malwares seront tenus sous contrôle via des machines virtuelles.