MALWARES : DÉTECTION, IDENTIFICATION ET ÉRADICATION V2

Apprenez à connaître les malwares, leurs grandes familles, à les identifier et à les éradiquer !

Cette formation permettra de comprendre le fonctionnement des malwares, de les identifier et de les éradiquer proprement, en assurant la pérennité des données présentes sur le SI. Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation, et mis en pratique lors des travaux dirigés.

Code : MDIEv2

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : Les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Introduction aux malwares
- Virus
- Vers
- Botnet
- Rançongiciels
- Rootkits (userland – kernel-land)
- Bootkit

Éradication
- Processus inforensique et analyse de logiciels malveillants
- Réponse aux incidents automatisée sur un parc

JOUR 2

Détection
- Les anti-virus et leurs limites
- Chercher des informations sur un malware
- NIDS / HIDS
- EDR
- Concept d'IOC dans le cadre d'un SOC / CERT (hash, motifs, etc.)

JOUR 3

Identification
- Analyse dynamique manuelle
- Analyse dynamique automatisée (sandboxes)
- Analyse statique basique
- Introduction à l'analyse mémoire avec Volatility
- Introduction à la rétro-conception

PROCHAINES DATES

1 février 2023,
11 avril 2023,
14 juin 2023,
4 septembre 2023,
6 novembre 2023

OBJECTIFS

- Reconnaître les mécanismes de dissimulation de malwares et mettre en place un environnement infecté
- Utiliser différents outils de détection de malware
- Mettre en place un système de collecte d'information
- Réaliser une rétro-ingénierie sur un malware
- Prendre en main les outils d'analyse dynamique
- Comprendre les mécanismes de persistance d'un malware

INFORMATIONS GÉNÉRALES

Code : MDIEv2
Durée : 3 jours
Prix : 2 400 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)

PUBLIC VISÉ

- Responsables gestions des incidents
- Techniciens réponse aux incidents
- Auditeurs techniques, Analystes de sécurité

PRÉ-REQUIS

- Notions de sécurité informatique
- Maîtriser les systèmes Windows et Linux
- Avoir des connaissances en protocoles réseaux TCP/IP
- Avoir des connaissances en développement

RESSOURCES

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne / Internet