EduGroupe
Accompagner pour réussir

Malwares : détection, identification et éradication

Référence : **SECMALWARE** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances du Système Microsoft Windows

Profil des stagiaires

- Auditeurs techniques, Analystes de sécurité
- Responsables gestion incident
- Techniciens réponse incident

Objectifs

- Connaitre les différents malwares
- Identifier un malware
- Mettre en œuvre des contre-mesures adéquates
- Apprendre à manier les outils d'inspection du système

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Techniques Cybersécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. JOUR 1

-

2. Introduction aux malwares

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

3. Eradication réponse à incident

- Processus inforensique et analyste de logiciels malveillants
- Réponse à incident automatisée sur un parc

4. JOUR 2

-

5. 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.)

6. JOUR 3

-

7. Identification

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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.