Cyber Threat Intelligence : initiation au renseignement sur les menaces

Référence : **SECTHREAT** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissances de base dans le fonctionnement des systèmes d'information (système, réseau) et en sécurité informatique.. • Il est demandé aux stagiaires de se munir d'un ordinateur portable (config. minimum : i3 / 2Go Ram) équipé de : Maltego version community et Virtualbox.

PROFIL DES STAGIAIRES

• Analyste CERT/CSIRT. • Consultant en cybersécurité. • Opérateur SOC. • Responsable d'équipe sécurité souhaitant initier une capacité Threat Intel. • Responsable de la sécurité des systèmes d'information (RSSI).

OBJECTIFS

• Comprendre les différentes facettes de la Threat Intelligence (stratégique, tactique, opérationnelle & technique). • Appréhender le paysage des cybermenaces d'aujourd'hui. • Connaître les principaux modèles, référentiels, formats et concepts de la Threat Intelligence. • Maîtriser les bases de l'investigation et de l'analyse en Threat Intelligence. • Connaître les principaux outils et sources d'informations. • Comprendre les applications concrètes de la Threat Intelligence : détecter (SOC), répondre (CERT/CSIRT) et « chasser » les incidents (hunting).

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un 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, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

JOUR 1

- La menace
- Le Renseignement
- Le cycle du Renseignement
- Les 3 domaines du Renseignement
- Sources
- Renseignement Appliqué
- Outillage
- Méthodes d'analyse
- Training - jour 1

JOUR 2

- Lecture : Draw me like one of your French APTs
- OPSEC
- Particules élémentaires de la CTI
- Exploitation des particules élémentaires en OSINT
- Modélisation des modes opératoires adverses
- Attribution
- Connecting the dots
- Training - Jour 2

JOUR 3

- Lecture : Pyschology of Intelligence Analysis - Richard Heuer
- Techniques d'Analyse Structurée
- Matrice d'hypothèses comparées (ACH)
- Biais cognitifs et erreurs de logique
- Techniques de manipulation de l'information
- Restitution et Diffusion du Renseignement
- Partage du Renseignement Technique
- Training - Jour 3