MAJ 07/11/2024

Formation « OSINT »

Réf : OSINT

Objectifs

- Réaliser des recherches avancées en source ouverte
- Rédiger des fiches opérationnelles du mode opératoire de l'attaquant
- Lier des identifiants à une ou des personnes physiques
- Mettre en place une stratégie de veille afin de suivre des attaquants ou de protéger une entreprise

Durée & horaires

- 4 jours soit 28 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Analyste SOC
- Enquêteur
- Analyste Threat Intel (CTI)
- Pentesteur

Pré-requis

- familiarité avec les réseaux sociaux facebook, twitter, instagram
- familiarité avec l'utilisation d'un terminal, notamment l'installation et l'utilisation d'outils en python
- familiarité avec github
- familiarité avec la CTI (sans forcément y travailler, au moins connaître les enjeux du métier)

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Immersion dans le rôle d'un enquêteur suite à une compromission
- Apprentissage par application concrète tout en laissant une grande autonomie dans la démarche d'investigation

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyée avant le début de la formation
- Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques
- Examen final à la fin de la formation (cf certification)

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification OSINT1 par HS2.**

Programme

- Méthodologie d'enquête (timeline, prise de note)
- Relevé d'Indice de Compromission (IoC)
- Pivot vers de nouveaux IoCs
- Recherche avancée : expression régulière (regexp)

- Moteur de recherche DeepWeb
- Dorking
- Cartographie réseau
- Renseignement sur protocoles variés (hors Web)
- Exploitation des métadonnées fichiers et protocoles

- Recherche et analyse de code
- Reverse image
- Utilisation outil open-source
- Reconnaissance réseau
- Outil d'investigation d'adresse courriel
- Cartographie d'information

Dates de nos prochaines sessions disponibles sur la page :
https://www.hs2.fr/osint