MAJ 08/03/2023

Formation « Détection et réponse aux incidents de sécurité avancée »

Réf : SECUBLUE2

Objectifs

- Enrichir une infrastructure de détection en place
- Appliquer la notion de "prévention détective"
- Identifier des chemins de compromissions potentielles
- Traiter une réponse à incident impliquant un nombre important de machine
- Mettre en œuvre des mesures de recherche de compromission

Durée & horaires

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

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Membres d'un SOC ou d'un CSIRT
- Administrateurs
- Responsables sécurité
- Concepteur / architecte de supervision

Pré-requis

- Avoir suivi la formation SECUBLUE1
- (ou) Solide expérience dans un SOC ou un CSIRT

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours en français au format papier en présentiel et au format numérique en distanciel
- 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

Certification

- A 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 SECUBLUE2 par HS2.

Programme

Détection réseau (1 journée)

- Configuration du pare-feu local pour la détection d'activité malveillante
- Recherche de canaux de communication avec l'infrastructure de l'attaquant (beaconing et exfiltration)

Détection système (0,5 journée)

- Détection des persistances
- Exploitation des quarantaines des anti-virus
- Détection d'exfiltration par USB (scénario DLP)

Chemins de contrôle Active Directory (0,5 journée)

- Détection de la collecte des informations
- Recherche d'événement typique d'une exploitation de chemins de contrôle

Réponse à incident (1,5 journée)

- Utilisation de l'outil de collecte DFIR-ORC (configuration et déploiement)
- Analyse des résultats de la collecte unitaire
- Recherche à large parc