Formation « Détection et réponse aux incidents de sécurité »

Réf : SECUBLUE

Les rapports de tous les grands acteurs de la réponse à incident sont unanimes : les compromissions, qu'elles soient l'œuvre de simples malwares ou de groupes organisés, sont légions, avec bien souvent un délai effarant de plusieurs mois entre l'arrivée de l'acteur malveillant et sa détection par les défenseurs. Dans ce contexte, la question n'est plus de savoir si cela peut nous arriver, mais bien QUAND cela va-t-il nous arriver ; L'enjeu n'est plus seulement de prévenir, mais d'aller traquer l'attaquant sur nos systèmes et réseaux afin de l'empêcher d'étendre son emprise et d'atteindre ses objectifs.

En mettant l'accent sur la compréhension des techniques d'attaque et la maitrise des outils de détection, cette formation vous donnera les moyens de tirer le meilleur parti des mesures et équipements déjà en place pour répondre rapidement et efficacement aux incidents de sécurité.

Objectifs

- Mettre en place une architecture de détection
- Appliquer la notion de "prévention détective"
- Limiter l'impact d'une compromission
- Prioriser les mesures de surveillance à implémenter
- Maitriser le processus de réponse à incident

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Membres d'un SOC ou d'un CSIRT
- Administrateurs
- Responsables sécurité

Pré-requis

- Formation SECUCYBER
- (ou) Solides bases en sécurité des systèmes d'information

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**
- **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

- **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 SECUBLUE par HS2.**

Programme

Module 1 : État des lieux

- Pourquoi la détection
  - Défense en profondeur
  - Tous compromis
- Évolution de la menace
- Principes de défense
- CTI et renseignement
  - IOC, Yara, MISP

Module 2 : Comprendre l'attaque

- Objectifs de l'attaquant
- Phases d'une attaque
- Plusieurs champs de bataille
  - Réseau
  - Applications
  - Systèmes d'exploitation
  - Active Directory
  - Utilisateurs et Cloud
- Portrait d'une attaque réussie

Module 3 : Architecture de détection

- Architecture sécurisée
- Détection : les classiques
  - IDS/IPS
  - SIEM
  - SandBox
  - Capture réseau
  - WAF
- Valoriser les "endpoints"
  - Whitelisting
  - Sysmon
  - Protections mémoire
  - Mesures complémentaires de Windows 10
- Les outsiders
  - "Self-defense" applicative
  - Honey-*
  - Données DNS
- Focus : Journalisation

Module 4 : Blue Team vs. attaquant

- Gérer les priorités
- Outils & techniques
  - Wireshark / Tshark
  - Bro / Zeek
  - Recherche d'entropie
  - Analyse longue traîne
- Détection et kill chain
  - Focus: Détecter Bloodhound
  - Exploitation
  - C&C
  - Mouvements latéraux
  - Focus : Attaques utilisant Powershell
  - Elévation de privilèges
  - Persistance
- Focus: détecter et défendre dans le Cloud

Module 5 : Réponse à incident et Hunting

- Le SOC & CSIRT
- Triage
- Outils de réponse
  - Linux
  - Windows
  - Kansa
  - GRR
- Partons à la chasse
  - Principes de base
- Attaquer pour mieux se défendre

- Audit "Purple team"