G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Détection et réponse aux incidents de sécurité

But de la formation

- 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
- Maîtriser le processus de réponse à incident

Pré-requis

- Formation "Fondamentaux techniques de la cybersécurité"
- (ou) Solides bases en sécurité des systèmes d'information

Type de public

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

Moyens pédagogiques

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

Sanction de la formation

- 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,
- Examen de certification HS2
- Formation délivrée en partenariat avec HS2

Méthodes pédagogiques

- Cours magistral avec travaux pratiques et échanges intéractifs

Durée

35 heures (5 jours).

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"