Détection et réponse aux incidents de sécurité

Référence : **SECBLUE** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir de solides bases en sécurité des systèmes d'information.

PROFIL DES STAGIAIRES

• 1-Membres d'un SOC ou d'un CSIRT. • 2-Administrateurs. • 3-Responsables 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.

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

État des lieux

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

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

Architecture de détection

- Architecture sécurisée
- Détections, 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

Blue Team vs. attaquant

- Gérer les priorités
- Outils & techniques : Outils & techniques ; Bro / Zeek ; Recherche d'entropie ; Analyse longue traîne
- Détection et kill chain
- Focus: détecter et défendre dans le Cloud

Réponse à incident et Hunting

- 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 »