Parcours métier d'Analyste SOC (Security Operations Center)

Référence : **SECSOC** Durée : **8 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi le parcours introductif à la Cybersécurité ou posséder les connaissances équivalentes. • Connaitre le guide d'hygiène sécurité de l'ANSSI.

PROFIL DES STAGIAIRES

• Administrateurs Systèmes et Réseaux. • Architectes réseaux. • Chefs de projets. • Consultants en sécurité. • Ingénieurs / Techniciens et Responsables techniques. • Responsables informatiques.

OBJECTIFS

• Comprendre comment durcir les systèmes d'exploitation. • Apprendre les défenses du périmètre pour analyser et attaquer ses propres réseaux. • Apprendre diverses techniques telles que l'ingénierie sociale, la détection d'intrusion. • Apprendre à gérer une variété d'incidents. • Configurer l'analyse de vulnérabilité. • Configurer les mises à jour de signature. • Comprendre l'analyse des logs.

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

Jour 1

- Définition et objectif d'un SOC
- Les métiers du SOC
- Catalogue de services et fonctions d'un SOC : Fonction de prévention de sécurité - Fonction de détection - Fonction de réaction
- Structure et fonctionnement d'un SOC : Processus du SOC - Ressource humaine - Structure de pilotage
- Les moyens : Humain - Logistique - Applicatif

Jours 2 -3 - 4

- Composants et architecture technique d'un SOC : Firewall / Proxy - IPS/IDS - Scan de vulnérabilités - SIEM - Les différents systèmes

Jour 5

- Les aspects juridiques d'une MOE d'un SOC
- Mise en place d'un SOC : Phase de conception : DESIGN - Phase de construction : BUILD - Phase de démarrage : RUN - Premier bilan

Jour 6

- Le contrôle et les indicateurs
- L'amélioration continue
- Le PCA PRA du SOC

- Relation avec les clients et les fournisseurs
- Externaliser le SOC

Jours 7- 8

- Etude sur un SOC existant

Dates de formation

- Du 14 au 15 Septembre et du 28 au 29 Septembre + du 12 au 13 Octobre et du 26 au 27 Octobre
- Du 05 au 06 Novembre + du 16 au 17 Novembre + du 26 au 27 Novembre + du 03 au 04 Décembre