

Parcours métier d'Analyste SOC (Security Operations Center)

Référence : **SECSOC**

Durée : **8 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- 1-Avoir suivi le parcours introductif à la Cybersécurité ou posséder les connaissances équivalentes. • 2-Connaître 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 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 des compétences acquises envoyée au stagiaire
- 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 ET 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 ET 8

- Etude sur un SOC existant

Dates des sessions de formation analyste SOC

- 23,24 juin + 03, 04, 10, 11, 24 et 25 juillet 2025
- 15, 16, 25, 26, 29 et 30 septembre + 09 et 10 octobre 2025
- 20, 21, 27 et 28 octobre + 03, 04, 24 et 25 novembre 2025

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.