

Certified Soc Analyst (certification comprise)

Référence : **SECCSA**

Durée : **3 jours (21 heures)**

Certification : **Oui**

Connaissances préalables

- 1-Avoir des connaissances en gestion d'incidents
- 2-Savoir ce qu'est un SOC

Profil des stagiaires

- 1-Analystes SOC (Niveau I et Niveau II)
- 2-Administrateurs de Réseau et Sécurité, Ingénieurs de Réseau et Sécurité, Analyste en Sécurité, Analystes en Défense de Réseau, Techniciens en Défense de Réseau, Spécialistes en Sécurité de Réseau, Opérateur en Sécurité de Réseau, et tout professionnel e
- 3-Analystes en Cybersécurité
- 4-Professionnels cybersécurité débutants
- 5-Quiconque voulant devenir Analyste SOC

Objectifs

- Comprendre le processus SOC de bout en bout
- Détecter des incidents avec un SIEM
- Détecter des intrusions avec les modèles de menace
- Comprendre le déploiement d'un SIEM

Certification préparée

Certified SOC Analyst. L'examen consiste en un QCM de 100 questions et dure 3 heures. Pour obtenir la certification vous devez avoir 70% de bonnes réponses

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation 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

1. Security Operations and Management

-

2. Understanding Cyber Threats, IoCs, and

-

3. Incidents, Events, and Logging

-

4. Incident Detection with Security

-

5. Enhanced Incident Detection with

-

6. Incidence Response

-

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel: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.