Analyste SOC (Security Operations Center)

Référence : **SECSOCB** Durée : **8 jours (56 heures)** Certification : **Aucune**

Connaissances préalables

- Avoir des connaissances en réseau
- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes

Profil des stagiaires

- Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets…

Objectifs

- Connaître le rôle et les missions d'un analyste SOC
- Maîtriser les fondamentaux de la cybersécurité défensive
- Utiliser les outils et technologies du SOC
- Analyser et corréler les événements de sécurité
- Gérer les incidents de sécurité
- Rédiger des rapports techniques
- Travailler en coordination avec les autres équipes de cybersécurité
- Faire de la veille (cybermenaces, techniques d'attaques)

Certification préparée

- Aucune

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Apports théoriques illustrés d'exemples concrets
- Exercices pratiques
- Étude de cas fil rouge
- Accès à une documentation pédagogique numérique
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation
- Possibilité de choisir entre 8 jours consécutifs ou un découpage(5+3) incluant des intersessions d'une à deux semaines

Formateur

- Consultant-formateur Analyste SOC

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire

- Attestations des compétences acquises et de fin de stage adressée à chaque participant

Contenu du cours

JOUR 1 – Introduction au SOC et missions de l'analyste (7h00)

• Définition et rôle d'un SOC
• Métiers et niveaux (N1, N2, N3, CTI, ingénierie SOC)
• Services et missions : prévention, détection, réaction
• Organisation : processus, ressources humaines, gouvernance SOC
• 🛠 Atelier : Cartographie des rôles et responsabilités dans un SOC fictif

JOUR 2 – Fondamentaux de la cybersécurité défensive (7h00)

• Principes : CIA, défense en profondeur, durcissement systèmes
• Menaces courantes : malware, phishing, ransomware, APT
• Outils de défense périmétrique : firewall, proxy, IDS/IPS
• Gestion des vulnérabilités : scans, patch management
• 🛠 Scan de vulnérabilités + analyse des résultats

JOUR 3 - Technologies du SOC : SIEM, EDR et monitoring (7h00)

• Architecture technique d'un SOC : SIEM, EDR, sondes, threat intel feeds
• Fonctionnement d'un SIEM : logs, parsing, règles de corrélation
• Introduction aux EDR (alertes comportementales)
• Cas d'usage : brute force, malware, anomalies réseau
• 🛠 TP : Exploration d'un SIEM (Splunk/ELK/QRadar) – recherche d'événements suspects

JOUR 4 - Analyse et corrélation des événements (7h00)

• Cycle de vie d'un événement dans le SOC
• Corrélation et enrichissement (IOC, MITRE ATT&CK)
• Gestion des faux positifs / faux négatifs
• Construction de use cases SOC
• 🛠 TP : Corrélation d'événements multiples et investigation guidée dans un SIEM

JOUR 5 - Gestion des incidents de sécurité (7h00)

• Typologie des incidents (phishing, ransomware, exfiltration)
• Processus de gestion : détection, qualification, escalade, containment, remédiation
• Coordination avec CSIRT, CERT et autres équipes (forensic, réseau, sécurité)
• Communication et reporting en situation de crise
• 🛠 Exercice : Simulation d'un incident phishing + qualification/escalade

JOUR 6 - Pratique incident response (7h00)

• Scénarios d'attaque réalistes : brute force, ransomware, exfiltration
• Identification des IOC (hash, IP, domaines malveillants)
• Analyse de journaux Windows/Linux, PCAP, EDR
• Plan de remédiation et bonnes pratiques
• 🛠 TP fil rouge : investigation complète d'un incident simulé avec restitution intermédiaire

JOUR 7 - Reporting et communication SOC (7h00)

- Structuration des rapports SOC : fiches d'incident, rapports journaliers/hebdomadaires
- Priorisation et scoring (CVSS, impact métier)
- Recommandations techniques et opérationnelles
- Communication adaptée (RSSI, direction, clients)
- 🛠️ Atelier : Rédaction d'un rapport d'incident + restitution orale en groupe

JOUR 8 -Veille et amélioration continue du SOC (7h00)

- Cyber Threat Intelligence et veille opérationnelle
- Sources : CERT, ANSSI, MITRE ATT&CK, IOC feeds, OSINT
- Intégration d'IOC dans le SIEM/EDR
- Amélioration continue (KPIs, SOC maturity model, retour d'expérience)
- 🛠️ Atelier : Mise en place d'un tableau de veille cyber + enrichissement d'un scénario de détection avec IOC

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