Cybersécurité

Analyste SOC (Security Operations Center)

A l'issue de la formation, le stagiaire sera capable d'assurer les fonctions d'analyste d'un Security Operations Center (SOC), principalement la détection et l'analyse des intrusions, l'anticipation et la mise en place des protections nécessaires.

Public visé

- Techniciens et administrateurs Systèmes et Réseaux,
- Responsables informatiques,
- Consultants en sécurité,
- Ingénieurs,
- Responsables techniques,
- Architectes réseaux,
- Chefs de projet

Les objectifs de la formation

- 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)

Les prérequis de la formation

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

Méthodes pédagogiques

- Apports théoriques structurés, illustrés par des exemples concrets et adaptés au contexte professionnel des participants.
- Exercices pratiques et ateliers à chaque étape pour favoriser l'appropriation des connaissances.
- Étude de cas permettant de relier les différents blocs de compétences.
- Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges plus concrets, en corrélation avec les attentes des stagiaires.
- Documentation pédagogique complète, fournie au format numérique.
- Questionnaire d'évaluation du cours en fin de formation, analysé par notre équipe pédagogique.
- Attestation des compétences acquises transmise au stagiaire à l'issue de la formation.
- Attestation de fin de formation adressée en même temps que la facture à l'entreprise ou à l'organisme financeur, confirmant la participation complète du stagiaire à la session.

Programme de la formation

Jour 1 :
- Introduction au SOC et à ses missions

Jour 2 :
- Défenses périmétriques et systèmes de détection

Jour 3 :
- Gestion des vulnérabilités

Jour 4 :
- SIEM et supervision de la sécurité

Jour 5 :
- Mise en place et aspects juridiques

Jour 6 :
- Pilotage, indicateurs et continuité

Jour 7 :
- Étude de cas

Jour 8 :
- Simulation et clôture de formation