Cybersécurité

Parcours introductif à la Cybersécurité

A l'issue de la formation, le stagiaire sera capable de mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.

Public visé

- Toutes personnes souhaitant s'orienter vers les métiers de la cybersécurité, notamment les techniciens et administrateurs systèmes et réseaux.

Les objectifs de la formation

- Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème…)
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Appréhender les métiers liés à la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifier les bonnes pratiques en matière de sécurité informatique.

Les prérequis de la formation

- Avoir des connaissances générales dans les systèmes d'information et connaître le guide d'hygiène sécurité de l'ANSSI.

Méthodes pédagogiques

- Apports théoriques structurés, illustrés par des exemples concrets et adaptés au contexte professionnel des participants.
- Exercices pratiques à chaque étape pour favoriser l'appropriation des connaissances.
- Étude de cas permettant de relier les différents blocs de compétences.
- 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 :
- **Matin :** Introduction et enjeux de la cybersécurité
- **Après-midi :** Panorama des menaces et principes fondamentaux

Jour 2 :
- **Matin :** Connaissance et sécurisation du Système d'Information
- **Après-midi** : Mesures de protection et supervision

Jour 3 :
- **Matin :** Introduction à la sécurité offensive
- **Après-midi :** Méthodologie des tests d'intrusion

Jour 4 :
- **Matin :** Phase de reconnaissance
- **Après-midi :** Reconnaissance active

Jour 5 :
- **Matin :** Techniques d'attaque avancées
- **Après-midi :** Exploitation et post-exploitation

Jour 6 :
- **Matin :** Sécurité du réseau
- **Après-midi :** Segmentation et filtrage

Jour 7 :
- **Matin** : Cryptographie appliquée
- **Après-midi :** Protocoles sécurisés

Jour 8 :
- **Matin :** Hardening systèmes
- **Après-midi :** Hardening Windows et réseaux

Jour 9 :
- **Matin :** Gouvernance et normes
- **Après-midi :** Politiques et métiers de la cybersécurité

Jour 10 :
- **Matin :** Tendances et avenir de la cybersécurité
- **Après-midi :** Mise en situation finale, restitution et évaluation finale