Formation **Cybersécurité : les fondamentaux**

Cette formation de cinq jours sur les fondations de la cybersécurité offre une introduction complète aux concepts, pratiques et enjeux actuels de la sécurité informatique. Elle est conçue pour fournir aux participants une compréhension approfondie des principes de base de la cybersécurité, incluant la gestion des risques, la législation en vigueur, ainsi que les stratégies de défense et d'attaque. En alliant théorie et pratique, les apprenants découvriront comment identifier et prévenir les cybermenaces, protéger les données sensibles, et mettre en œuvre des solutions de sécurité adaptées aux environnements professionnels. Ce programme est idéal pour ceux souhaitant acquérir ou renforcer leurs compétences en cybersécurité dans un contexte professionnel.

Durée
5 jours

Objectifs pédagogiques

- Appréhender les notions fondamentales de la cybersécurité
- Identifier et analyser les menaces et vulnérabilités
- Maîtriser la législation et la conformité en cybersécurité
- Découvrir les techniques offensives et préventives
- Appliquer les stratégies de défense et de sécurisation des données
- Évaluer les risques et mettre en place des contre-mesures

Public
Tous

Prérequis
Avoir des connaissances de base en informatique (réseaux, systèmes d'exploitation, etc.). Une expérience professionnelle dans le domaine IT est recommandée mais non obligatoire.

Programme de formation

Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

Introduction à la cybersécurité : comprendre les enjeux

Définition et périmètre de la cybersécurité
Les axes stratégiques de sécurité
Gouvernance et cybersécurité : alignement avec les enjeux organisationnels
La cybersécurité par le droit : privacy, RGPD, NIS2, HDS

Les principes clés de la cybersécurité

Le Kernel Protection : rôle et importance
Notions fondamentales de traçabilité et sauvegardes
Sécurité de la donnée et sécurité physique
Gestion des accès : authentification et chiffrement

Analyser les risques et protéger les systèmes

Introduction à la gestion des risques : SMSI et AMDEC
Exercice pratique : évaluation des risques et mise en place de contre-mesures
Comprendre une faille et son exploitation (CVE)
Approche préventive et gestion de crise

Comprendre et neutraliser les menaces

Approche offensive : dans la tête des attaquants
Différentes techniques d'attaques
Social Engineering : phishing (mail, QR, scam…)
Attaques MITM : principes et défenses
Renseignements : reconnaissance passive et active

Approche défensive : bâtir des remparts solides
Évaluation des vulnérabilités et outils associés
Surface d'attaque et politique du « juste nécessaire »
Hardening, tiering et tracing : renforcer vos défenses

Piloter la cybersécurité au quotidien

Rôle et missions d'un SOC (Security Operations Center)
CERT (Computer Emergency Response Team) : anticipation et réponse
Criminalistique numérique : investiguer efficacement après une attaque
Mise en place d'une politique de sécurité globale

Exemples d'ateliers et études de cas

Étude approfondie d'une attaque type et ses impacts
Simulations de phishing et reconnaissance
Élaboration d'une stratégie de sauvegarde et de récupération
Analyse en temps réel d'une surface d'attaque et ajustements en direct

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.