

Cybersecurite - Les fondamentaux

CYBERFOND

Cette formation vise à fournir une compréhension approfondie des concepts fondamentaux en cybersécurité, en mettant l'accent sur les menaces, les risques et les meilleures pratiques pour protéger les données et les systèmes informatiques. Les participants apprendront les principes de base de la sécurité informatique, les types de menaces courantes, les techniques de protection et les stratégies de prévention des attaques.

Présentiel - Synchron

Objectifs

Public Visé

Employés des services informatiques et technologiques, Responsables de la sécurité informatique, Analystes en sécurité informatique, Administrateurs système, Ingénieurs en sécurité, Développeurs de logiciels, Gestionnaires de réseau, Professionnels des technologies de l'information (TI), Cadres et dirigeants soucieux de la sécurité des données de leur entreprise.

Pré Requis

Posséder des bases dans la sécurité des systèmes d'information. Connaître le fonctionnement d'un réseau, maîtriser des connaissances dans la gestion des données et de leur circulation.

Objectifs pédagogiques et d'évaluation

Comprendre les bases de la cybersécurité, le profil des interlocuteurs et le cadre de gouvernance nécessaire pour les entreprises
Maîtriser les types menaces au niveau des systèmes d'information et les pratiques d'hygiène de base en matière de cybersécurité
Comprendre les étapes d'évaluation des risques cyber, les exigences légales et les différents niveaux de maturité cyber pour les entreprises
Introduire les méthodes de gouvernance et de mise en place des mesures de cybersécurité
Comprendre les fondamentaux et les mesures essentielles de cybersécurité à travers une étude de cas de bout en bout

Méthodes pédagogiques

Méthodes démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation)
Beaucoup de tests et d'exemples concrets en lien direct avec les besoins des participants
Des techniques directement mobilisables dans le cadre de leurs fonctions
Formation axée sur la mise en pratique
Méthode participative
Alternance de cours et d'exercices dirigés ou en autonomie
Travaux individuels et corrections collectives
Evaluation croisée et partage de bonnes pratiques

Moyens pédagogiques

En présentiel :

Parcours pédagogique

Jour 1 : Introduction à la cybersécurité et à la gouvernance

Aperçu de la cybersécurité : Objectifs, paysage des menaces et tendances
Aperçu des profils d'expertise en cybersécurité et domaines de connaissance
Introduction à la gouvernance en cybersécurité
Exemple de cas pratique

Jour 2 : Fondamentaux techniques de la cybersécurité

Introduction à l'architecture des systèmes d'information
Comprendre les réseaux et les services cloud
Vecteurs d'attaque et paysage des menaces
Pratiques d'hygiène de base en matière de cybersécurité

Jour 3 : Les risques de sécurité numérique et la réglementation

Identification et évaluation des risques cyber
Stratégies de gestion des risques cyber
Vue d'ensemble de la réglementation en matière de cybersécurité
Conformité et exigences légales pour les entreprises
Exemple de méthodes et outils

Jour 4 : Mise en œuvre et gestion des mesures de cybersécurité

Élaboration et mise en œuvre d'un plan de mesures proactives
Solutions et logiciels de cybersécurité
Planification et gestion de la réponse aux incidents
Cycle de gestion et d'amélioration continue

Jour 5 : Cas pratique traitant les fondamentaux de la cybersécurité

Evaluation du niveau de maturité en cybersécurité d'une petite entreprise
Elaboration d'un plan de mise en conformité et de gestion des risques
Elaboration d'un plan de mesures de cybersécurité

1 ordinateur par stagiaire
Salle de formation claire, climatisée et spacieuse
Tableau blanc
Vidéo projecteur
Support de cours
Environnement de formation installé sur les postes de travail ou en ligne

En distanciel :

Formation en distanciel via TEAMS. L'apprenant reçoit une invitation avec le lien de connexion. Le premier jour, le conseiller assure la présentation des personnes, de la formation, des outils d'émargement et d'évaluation puis le formateur prend le relai et démarre la formation. Le dernier jour, le conseiller procède à la clôture de la session avec le formateur et les apprenants.

Qualification Intervenant-e-s

Formateur - Consultant spécialisé dans la sécurité des systèmes d'information

Méthodes et modalités d'évaluation

- Questionnaire d'auto-positionnement - Evaluation en cours de formation : études de cas - Evaluation de fin de formation : Auto-évaluation/Quiz/Exercice d'application - Bilan individuel des compétences acquises - Questionnaire de satisfaction à chaud - Questionnaire de satisfaction à froid

Modalités d'Accessibilité

Pour les personnes en situation de handicap, nous consulter et, en fonction de vos besoins spécifiques, un entretien avec notre référente handicap sera organisé. Vous pourrez vous exprimer en toute confidentialité et liberté sur votre handicap.

 **Durée** **Effectif**
35.00 Heures **5** Jours De 3 à 8 Personnes

 **Contactez-nous !** **Stéphane POUILLOT** **Tél. : 0690371551**
Commercial **Mail : spouillot@strategie-info.com**