Formation **Gouvernance de la cybersécurité**

Ce cours immersif sur la gouvernance de la cybersécurité permet aux professionnels de la cybersécurité d'acquérir l'expertise nécessaire pour développer et gérer des cadres de gouvernance solides. Les participants acquerront des compétences en matière de gestion des risques, de conformité, de stratégies de sécurité et d'audits, en s'alignant sur les normes industrielles telles que ISO et NIST. Ce cours est conçu pour les professionnels expérimentés qui cherchent à améliorer leur savoir-faire en matière de gouvernance et à protéger efficacement leurs organisations.

Durée
1 jour

Objectifs pédagogiques

- Identifier les principaux cadres et normes de gouvernance tels que ISO, NIST et COBIT
- Comprendre les rôles et responsabilités dans la gouvernance de la cybersécurité
- Formuler des stratégies de sécurité efficaces
- Effectuer des évaluations approfondies des risques et mettre en place des processus de gestion des risques
- Évaluer la conformité et les obligations légales en matière de cybersécurité
- Connaître les pratiques de contrôle et d'audit en vue d'une amélioration continue

Public
Professionnels de la cybersécurité

Prérequis
Une base solide en matière de principes et de pratiques de cybersécurité. Il est recommandé de se familiariser avec les cadres et les normes de sécurité de base.

Programme de formation

Phase d'inclusion

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

Introduction à la gouvernance de la cybersécurité

Vue d'ensemble de la gouvernance de la cybersécurité
Importance dans le contexte organisationnel
Différences entre la gouvernance et la gestion
Principes fondamentaux de la gouvernance de la cybersécurité

Cadres et normes de gouvernance

Introduction à ISO 27001
Aperçu du cadre de cybersécurité du NIST
Examen du cadre COBIT
Comparaison entre les différents cadres

Rôles et responsabilités

Attribution des rôles dans la gouvernance de la cybersécurité
Principales responsabilités des parties prenantes
Avantages de structures de gouvernance claires
Importance du soutien des dirigeants

Stratégie et politiques de sécurité

Stratégie et politiques de sécurité
Principes essentiels d'une stratégie de sécurité
Alignement de la stratégie sur les objectifs de l'entreprise
Élaboration de politiques de sécurité
Mise en œuvre et maintien des politiques

Évaluation et gestion des risques

Comprendre les méthodes d'évaluation des risques
Identifier et évaluer les risques
Élaborer un plan de gestion des risques
Contrôler et atténuer les risques en permanence

Conformité et obligations légales

Vue d'ensemble des réglementations en matière de cybersécurité
Identifier les exigences juridiques applicables
Garantir le respect des normes
Implications juridiques des atteintes à la cybersécurité

Contrôle de la sécurité et audits

Mise en place de processus de surveillance
Réalisation d'audits internes efficaces
Rôle des audits externes dans la conformité
Amélioration continue grâce aux audits

Meilleures pratiques et études de cas

Examen des meilleures pratiques en matière de cybersécurité
Apprentissage à partir d'études de cas de l'industrie
Adaptation des meilleures pratiques à des environnements spécifiques
Création d'une culture de la sécurité

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.