Management stratégique en cybersécurité

Description de la formation

La formation Management Stratégique en Cybersécurité est une formation immersive conçue pour les dirigeants, managers et responsables de la sécurité souhaitant aligner la cybersécurité sur la stratégie globale de leur organisation. Elle fournit les clés pour comprendre l'environnement métier, évaluer les menaces et construire une stratégie cyber cohérente, mesurable et communicable. À travers des études de cas, des outils éprouvés (BMC, SWOT, NIST, MITRE…), et des mises en situation, les participants acquièrent une vision stratégique et opérationnelle de la cybersécurité, intégrant la gouvernance, la communication et le pilotage par la valeur.

Objectifs pédagogiques

- Comprendre l'environnement métier, stratégique et les enjeux de la cybersécurité à l'échelle d'une organisation.
- Identifier les parties prenantes et construire une cartographie d'acteurs.
- Analyser les menaces, les vulnérabilités et les risques à un niveau stratégique.
- Concevoir un plan stratégique de cybersécurité aligné avec les objectifs métier.
- Définir une gouvernance cyber efficace et piloter la sécurité par les indicateurs.
- Élaborer et piloter des politiques de sécurité structurées autour de principes, normes et procédures.
- Communiquer efficacement la stratégie cybersécurité auprès de la direction générale et des équipes.

Prérequis

- Connaissance de base en systèmes d'information.
- Sensibilité aux enjeux de la cybersécurité.
- Expérience professionnelle en management souhaitée.

Modalités pédagogiques

- **Modalité :** Formation réalisée en présentiel.
- **Méthode :** La formation se déroule entre 50% de théorie et 50% de pratique. Le formateur partage des points théoriques et des cas concrets, lance des discussions et échanges entre les stagiaires et propose des jeux / outils en relation avec le contenu et des mises en pratique.
- **Support de formation :** Le support de formation utilisé par le formateur est remis au stagiaire à l'issue de la formation.

Modalités techniques

- En format présentiel, le formateur dispose d'une présentation (support de formation), d'un vidéoprojecteur (ou TV), de tableaux blancs et de jeux / d'outils pédagogiques.
- En format présentiel, le stagiaire n'a besoin d'aucun support particulier pour suivre la formation.

Code

CYB100

Durée

3 jours (21 heures)

Nombre de participants

Entre 3 (minimum) et 12 (maximum) participants.

Profil des stagiaires

Cadres dirigeants, Responsables de la sécurité de l'information, Directeurs des Systèmes d'Information et Chef de projet IT et Cybersécurité.

Sanction de la formation

Attestation de fin de formation.

Accessibilité

Accessible pour les personnes en situation de handicap et aménagement possible en fonction du type de handicap (prévenir avant le début de la formation).

Modalités et délais d'accès

10 jours minimum avant la formation pour une demande de prise en charge.

Modalités de suivi et d'évaluation

- Evaluation préalable.
- Evaluation de fin de formation sous forme de test (QCM) afin de valider l'acquisition des compétences et des connaissances.
- Questionnaire d'évaluation de la satisfaction en fin de formation.
- Feuille d'émargement signée par le(s) stagiaire(s) et le formateur, par demi-journée de formation.
- Attestation de fin de formation.
- Evaluation de suivi à froid (+ 1 mois).

Intervenant

Nos formateurs sont **experts en cybersécurité, RSSI et/ou ancien responsable de cybersécurité pour des grands groupes**. Ils accompagnent à tous les niveaux de l'organisation et sont passionnés par le monde de la cybersécurité.

Tarifs

- Interentreprises : 4 500,00 € HT
- Intra-entreprise : sur demande

Contenu de la formation

JOUR 01

INTRODUCTION

- Accueil des stagiaires
- Présentation du déroulement de la formation
- Les attentes

CYBERSÉCURITÉ ET STRATÉGIE D'ENTREPRISE

Objectif : Comprendre les enjeux business et leur articulation avec la stratégie de cybersécurité.

- **Analyse du contexte stratégique de l'entreprise :** business model, objectifs organisationnels, environnement concurrentiel.
- **Alignement cybersécurité / stratégie business :** comment la cybersécurité soutient les finalités stratégiques.
- **Analyse des menaces :** identification des risques internes/externes et compréhension du paysage de la menace.

JOUR 02

ACCUEIL

- Retour sur le jour 01

ÉLABORATION DE LA STRATEGIE CYBERSECURITE

Objectif : Construire une stratégie cybersécurité intégrée, de l'évaluation à la gouvernance.

- **DEFINITION ET STRUCTURATION DES POLITIQUES :** exploration de la pyramide des politiques (principes, politiques, standards, procédures, lignes directrices).
- **PLANIFICATION STRATEGIQUE :** cadrage de la feuille de route, priorisation des initiatives.
- **DESIGN STRATEGIQUE :** articulation autour de Frameworks reconnus (NIST CSF, CIS Controls).
- **PILOTAGE DE LA STRATEGIE :** indicateurs (KPIs, tableaux de bord stratégiques, scorecards).

JOUR 03

ACCUEIL

- Retour sur le jour 02

ATELIER IMMERSIF : STRATEGIE EN ACTION

Objectif : Mettre en pratique les acquis en situation de simulation.

Les participants sont répartis par équipes et plongés dans un scénario d'entreprise fictive. Ils doivent,

- Analyser le contexte de l'entreprise et ses enjeux cyber.
- Concevoir une stratégie de cybersécurité réaliste et cohérente.
- Prioriser les actions, anticiper les risques et structurer la gouvernance.
- Présenter leur plan devant un "comité exécutif" incarné par les formateurs et experts.

CONCLUSION