Planification Stratégique de la Cybersécurité

Durée : **3** jours **Prix :** 3 160 € HT

Contexte

Malgré les efforts déployés par les organisations pour sécuriser leurs systèmes, le nombre d'attaques réussies est toujours en forte et constante augmentation. Cette situation peut s'expliquer en partie par le fait que nombreuses sont les organisations qui sont dans une démarche réactive et défensive.

Cette vision opérationnelle de la cybersécurité n'est pas sans inconvénients. Le premier inconvénient, et le plus important, confère le leadership aux cybercriminels. En effet, ce sont ces derniers qui vont orienter le comportement des organisations. Le second inconvénient est que trop de sécurité tue la sécurité. La peur d'être attaqué fait que les organisations vont se perdre dans la nébuleuse de solutions de protection proposées par le marché et chercher à empiler les solutions les unes sur les autres sans véritable cohérence.

Cette formation a pour but de permettre aux organisations de s'approprier le leadership en matière de cybersécurité d'une part ; et d'autre part d'inscrire la cybersécurité comme objectif stratégique de l'organisation.

La création d'un plan stratégique de cybersécurité permet d'établir une vision réaliste, claire, et résiliente pour protéger les actifs de l'organisation, faire face aux cybermenaces, et assurer la continuité d'activité de l'organisation même après une attaque réussie.

Objectifs

Cette formation vise à comprendre l'importance d'un plan stratégique de cybersécurité permettant ainsi de se mettre en action, de prendre de meilleure décision, de rallier les gens autour d'un projet commun et de stimuler l'engagement des parties prenantes.

Au terme de cette formation, le stagiaire sera en mesure :

- De comprendre l'importance de la mise en place d'un plan stratégique.
- D'identifier et de définir une vision de la cybersécurité.
- De prendre de meilleures décisions en matière de cybersécurité.
- D'évaluer le retour sur investissement de la cybersécurité.
- De comprendre la différence entre cybersécurité et cyber-résilience.
- De mettre en place un plan d'action de protection des actifs de l'organisation.

Public visé

Top Management, Managers, Responsables de la sécurité des systèmes, Gestionnaires et Exploitants des Assets, Cadres et toute personne intéressée par la stratégie de cybersécurité.

Prérequis

Aucun.

Modalités pratiques

Méthodologie pédagogique

Exposé, échanges d'expérience, études de cas.

Méthodologie d'évaluation

Le stagiaire reçoit en amont de la formation un questionnaire permettant de mesurer les compétences, profil et attentes du stagiaire. Tout au long de la formation, les stagiaires sont évalués au moyen de différentes méthodes (quizz, ateliers, exercices et/ou de travaux pratiques, etc.) permettant de vérifier l'atteinte des objectifs. Un questionnaire d'évaluation à chaud est soumis à chaque stagiaire en fin de formation pour s'assurer de l'adéquation des acquis de la formation avec les attentes du stagiaire. Une attestation de réalisation de la formation est remise au stagiaire.

Programme

Module 1 : concepts fondamentaux de la planification stratégique

- La vision.
- La mission.
- Le contexte.
- Les enjeux.
- Les principales fonctions de la planification stratégique.
- Les fonctions qui alimentent le cycle de gestion.
- Les orientations stratégiques.
- Les axes d'intervention.
- Les objectifs de résultats.
- Les indicateurs de performance.
- Les tableaux de bord de pilotage.

Module 2 : les outils de la planification stratégique

- Effectuer un S.W.O.T. : forces/faiblesses/opportunités/menaces.
- Utiliser le S.T.E.E.P.L.E.
- Clarifier les objectifs en utilisant le modèle SMART.
- Utiliser le modèle ERAC : éliminer/réduire/augmenter/créer.
- Évaluation du ROI de la cybersécurité.

Module 3 : démarche de planification stratégique

- Généralités sur la démarche.
- Préparation de l'exercice.
- Réflexion et diagnostic
- Choix stratégiques.
- Mise en oeuvre du plan d'action.

Module 4 : l'évaluation de la maturité en cybersécurité

- L'approche horizontale avec le référentiel ISO 27001:2022.
- L'approche verticale avec CSF (Cyber Security Framework) du NIST.
- Déclinaison 360° du profil actuel de sécurité.
- Déclinaison 360° du profil souhaité de sécurité.

Module 5 : Cybersécurité - la sécurité construite à partir d'une démarche défensive et réactive

- Fondamentaux de la cybersécurité.
- Concepts et méthodes de la défense en profondeur.
- Bénéfices et limites de la cybersécurité dans la lutte contre la cybercriminalité.

Module 6 : Cyber-résilience - la sécurité construite à partir d'une démarche offensive et proactive

- Définition de la cyber–résilience.
- Concepts de la cyber–résilience.
- Démarche de mise en oeuvre de la cyber-résilience.