Développer les bonnes pratiques en matière de cybersécurité

La cyber délinquance a envahi notre quotidien. Jour après jour les médias nous annoncent des attaques de plus en plus pernicieuses. Nul ne peut se dire à l'écart de ces pratiques malveillantes et chacun peut se trouver confronté à des pertes de données.
Vol, panne de matériel, déni de services, cryptage de données, les risques sont présents pour toutes les entreprises. Il devient essentiel de définir une réelle politique de sécurité du système d'information adaptée à la structure de son entreprise.
Mettre en place des dispositifs techniques, former et sensibiliser ses collaborateurs, mettre en place une charge ou des plans de secours sont des actions qui permettront de limiter les risques et de gagner du temps en cas d'incident.
Cette formation a pour objectif de vous donner les éléments, bonnes pratiques et méthodes permettant de mettre en place une action de Sécurité des Systèmes d'Information dans votre entreprise.

Objectifs

- Identifier les différentes attaques de cyber sécurité
- Comprendre les enjeux et les impacts des attaques cyber sécurité.
- Appliquer les bonnes pratiques de gouvernance et de sécurité.

Prérequis

- Aucun pré-requis.

Public

- Tout employé d'une entreprise concerné par le développement des bonnes pratiques en matière de cyber sécurité.

Durée

- 1 journée : 9h00-17h00 - 7 heures
- Intégrant 1 pause matin et après-midi et pauses déjeuners

Déroulement pédagogique

Projection du cours sur vidéoprojecteur. Le support et la formation sont en langue française. Le support est livré sous PDF. Le cours est théorique à 70% et 30% pratique avec des discussions, partage d'expérience et étude de cas et quizz pour valider les acquis de formation. Une attestation de formation est délivrée en fin de formation.

Déroulement de l'examen

- Pas d'examen

Programme

La cybersécurité : Définition et notions de base : La sécurité des SI (prévention), La cyberdéfense (réaction), La cybercriminalité et cyberterrorisme (sanction) - Panorama des menaces selon une typologie - Les vulnérabilités (exemple, détermination, veille)- Identification et évaluation des actifs et des objectifs de sécurité- Les aspects juridiques et assurantielle (CNIL, RGPD)

Analyse de risques : Identifications des actifs- Identification des menaces et vulnérabilités- Calcul de risque- Remédiations - Evaluation de la sécurité – Supervision- Analyse dynamique de risque- Bonnes pratiques : Connaitre le SI et ses utilisateurs, Maitriser le processus et le réseau ,Mettre à niveau les logiciels, Authentification des utilisation, Problématiques liés au BYOD, Sécurisation des communications, Protection des données, Audit de lé sécurité :

Principes et domaines de la SSI afin de sécuriser les réseaux internes : Développement de la notion de défense en profondeur- Politique et stratégie de sécurité - Gestion des flux, notamment réseaux sans fil / architecture réseaux (cloisonnement du réseau) - Gestion des comptes, des utilisateurs, des privilèges selon le besoin d'en connaître - Gestion des mots de passe - Gestion des mises à jour - Journalisation et analyse - Gestion des procédures - Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA) - Virtualisation / cloisonnement - Détecter un incident - Gestion de crise :Traitement technique de l'incident , Procédure organisationnelle et communication , Reprise d'activité Méthodologie de résilience de l'entreprise - Méthodologie de résilience de l'entreprise - Outillages disponibles –

Se faire accompagner :les différentes formes d'externalisation, Comment choisir son prestataire de service, Présentation du référentiel de l'ANSSI, Présentation de la qualification SecNumCloud