Mise en Place de la Cybersécurité en Entreprise

Table des matières

Apport pour l'entreprise :

- **Protection des données et des systèmes** : Assurer la confidentialité, l'intégrité et la disponibilité des données critiques de l'entreprise.
- **Réduction des risques** : Identifier, évaluer et atténuer les risques de cyberattaques et de violations de données.
- **Conformité réglementaire** : Se conformer aux normes et réglementations en matière de protection des données (RGPD, ISO/IEC 27001, etc.).
- **Renforcement de la résilience** : Développer des capacités de réponse et de récupération rapide face aux incidents de sécurité.

Objectif de la formation : Outiller les participants pour qu'ils puissent développer, mettre en œuvre, et évaluer un programme complet de cybersécurité qui protège les actifs numériques de l'entreprise et soutient ses objectifs stratégiques.

Plan de formation détaillé :

Jour 1 : Introduction à la Cybersécurité et Évaluation des Risques

- **Objectifs** :
    - Comprendre les concepts fondamentaux de la cybersécurité et son importance pour l'entreprise.
    - Réaliser une évaluation des risques de cybersécurité spécifiques à l'entreprise.

- **Contenu** :
    - **Introduction générale** : Concepts clés de la cybersécurité, menaces courantes, importance pour l'entreprise.
    - **Évaluation des risques** : Méthodologies d'évaluation des risques (ISO 27005, NIST SP 800-30), identification des actifs critiques et des vulnérabilités.
    - **Cartographie des menaces** : Identification des menaces spécifiques à l'entreprise (phishing, ransomware, APT, etc.).
    - **Étude de cas pratique** : Évaluation des risques de cybersécurité pour une entreprise fictive ou réelle.

Jour 2 : Développement de la Politique de Sécurité de l'Information

- **Objectifs** :
    - Élaborer une politique de sécurité de l'information adaptée aux besoins et aux risques de l'entreprise.
    - Définir les rôles, responsabilités, et procédures de gestion de la sécurité.

- **Contenu** :
    - **Politique de sécurité de l'information** : Principes, objectifs, et portée de la politique, alignement avec les objectifs stratégiques.
    - **Gouvernance de la sécurité** : Mise en place d'un comité de sécurité, définition des rôles et responsabilités.
    - **Procédures de sécurité** : Élaboration de procédures pour la gestion des accès, la classification des informations, la gestion des incidents, etc.
    - **Atelier pratique** : Développement d'une politique de sécurité de l'information pour une entreprise spécifique.

Jour 3 : Mise en Place des Contrôles de Sécurité Techniques

- **Objectifs** :
    - Mettre en place des mesures techniques de sécurité pour protéger les systèmes, les réseaux et les données.
    - Utiliser les outils et technologies de cybersécurité pour renforcer la protection des actifs numériques.
- **Contenu** :
    - **Contrôles de sécurité techniques** : Firewall, antivirus, chiffrement, systèmes de détection/prévention d'intrusion (IDS/IPS), gestion des accès (IAM).
    - **Sécurisation des réseaux** : Segmentations réseau, VPN, sécurité Wi-Fi, protection contre les attaques DDoS.
    - **Sécurité des applications et des systèmes** : Gestion des patchs, sécurisation des serveurs et des applications web.
    - **Étude de cas** : Mise en œuvre de contrôles de sécurité techniques pour une entreprise fictive ou réelle.

Jour 4 : Sensibilisation et Formation des Utilisateurs

- **Objectifs** :
    - Développer un programme de sensibilisation et de formation à la cybersécurité pour tous les employés.

    - Assurer que les bonnes pratiques de sécurité sont comprises et suivies par l'ensemble du personnel.

- **Contenu** :
    - **Sensibilisation à la cybersécurité** : Importance de la sensibilisation, identification des menaces courantes pour les utilisateurs.
    - **Programme de formation** : Conception et mise en œuvre de formations sur les bonnes pratiques (mots de passe, phishing, utilisation des dispositifs mobiles).
    - **Campagnes de sensibilisation** : Organisation de campagnes régulières, simulations d'attaques (phishing, social engineering).
    - **Jeux de rôle** : Simulation d'une réponse à une attaque de phishing en entreprise.

Jour 5 : Gestion des Incidents de Sécurité et Plan de Continuité d'Activité

- **Objectifs** :
    - Mettre en place un processus de gestion des incidents de sécurité pour une réponse rapide et efficace.
    - Développer un plan de continuité d'activité (PCA) et un plan de reprise après sinistre (DRP) pour minimiser les impacts d'un incident majeur.

- **Contenu** :
    - **Gestion des incidents de sécurité** : Détection, classification, réponse, et analyse post-incident (CERT, SOC).
    - **Plan de continuité d'activité (PCA)** : Élaboration d'un plan pour assurer la continuité des opérations critiques en cas d'incident.
    - **Plan de reprise après sinistre (DRP)** : Stratégies pour la récupération des systèmes et des données après un incident majeur.
    - **Atelier pratique** : Élaboration d'un plan de gestion des incidents et d'un PCA pour une entreprise spécifique.

Jour 6 : Conformité et Audit en Cybersécurité

Jour 7 : Certification et Plan de Suivi Post-Formation

- **Objectifs** :
    - Valider les compétences acquises en cybersécurité et planifier un suivi post-formation pour assurer la pérennité des pratiques de sécurité.
    - Élaborer un plan de suivi pour garantir l'évolution continue des pratiques de cybersécurité.
- **Contenu** :
    - **Révision des concepts clés** : Récapitulatif des principaux apprentissages de la formation.
    - **Examen pratique** : Développement et évaluation d'un programme complet de cybersécurité pour une entreprise.
    - **Planification du suivi post-formation** : Définition des actions à suivre pour garantir l'efficacité continue des pratiques de cybersécurité.
    - **Cérémonie de remise des certifications** : Validation des compétences et remise des certificats de participation.
    - **Présentation des outils de suivi** : Accès à une plateforme en ligne, ressources supplémentaires, et soutien continu pour l'évolution des pratiques de cybersécurité.

Critères d'évaluation :

- **Examen pratique final** : Notation sur la capacité à concevoir, mettre en œuvre, et évaluer un programme de cybersécurité complet, incluant les politiques, les contrôles techniques, et la gestion des incidents.
- **Participation active** : Implication dans les discussions, études de cas, et jeux de rôle.
- **Travaux pratiques** : Qualité des politiques de sécurité développées, des contrôles techniques implémentés, et des plans de gestion des incidents proposés.

Accompagnement personnalisé :

Suivi Post-Formation :

- **1ère Visite de Suivi (1 mois après la formation)** : Vérification de la mise en œuvre des politiques et des contrôles de cybersécurité, ajustements si nécessaires.
- **2ème Visite de Suivi (3 mois après la formation)** : Évaluation de l'efficacité des pratiques de cybersécurité et identification des opportunités d'amélioration.
- **Support continu** : Assistance par e-mail ou téléphone, accès à une plateforme de ressources pour des questions spécifiques ou l'échange de bonnes pratiques.
- **Accès à une plateforme en ligne** : Documentation, guides pratiques, et forums de discussion pour soutenir l'évolution continue des pratiques de cybersécurité.

Ce plan de formation est conçu pour permettre aux participants de maîtriser toutes les étapes de la mise en place et de la gestion d'un programme de cybersécurité efficace, en répondant aux besoins spécifiques de l'entreprise cliente.