Maîtriser les enjeux et les fondamentaux de la cybersécurité

Acquérir les fondamentaux de la cybersécurité et comprendre les enjeux SSI en entreprise

Séminaire en présentiel
Sécurité

Code :
FXSSI

Durée :
2 jour(s) (14,00 heures)

Exposés : **40 %**
Cas pratiques : **40 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 120,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Dans un environnement organisationnel caractérisé par l'accroissement et la sophistication des cybermenaces, ce module vise à établir un socle partagé de connaissances en sécurité des systèmes d'information. Il a pour finalité de doter les participants des notions fondamentales de cybersécurité, d'expliciter la nature des risques numériques et de permettre l'identification des principales menaces susceptibles d'affecter l'entreprise.

La formation articule apports conceptuels, illustrations à partir de situations professionnelles et temps d'échanges afin de favoriser l'appropriation de bonnes pratiques mobilisables au quotidien, contribuant ainsi à la réduction de l'exposition aux risques et au renforcement de la posture de sécurité collective.

OBJECTIFS PEDAGOGIQUES

- Construire une culture commune en sécurité des systèmes d'information en identifiant les enjeux clés et en partageant des référentiels communs.
- Expliquer les concepts fondamentaux de la cybersécurité et les illustrer à travers des cas concrets
- Comprendre les risques numériques en identifiant les principales menaces et en évaluant leurs impacts sur un système d'information
- Appliquer les bonnes pratiques de sécurité au quotidien et adapter son comportement face à des situations à risque

PUBLIC CIBLE

- Ensemble des collaborateurs
- Collaborateur IT ou SSI (Débutant)
- Manager souhaitant comprendre les enjeux SSI

PRE-REQUIS

Aucun prérequis technique nécessaire

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

COMPRENDRE LES ENJEUX ET LES MENACES

- Introduction à la SSI et aux enjeux
  - Définition de la SSI
  - Les enjeux de la SSI pour l'entreprise et ses actifs (données, systèmes, utilisateurs, clients).
  - Les impacts d'un incident de sécurité (financiers, juridiques,réputation)
  - Exemples concrets d'incidents (fuites de données, ransomware, etc.)
- Principes fondamentaux de la sécurité
  - Confidentialité – Intégrité – Disponibilité – Traçabilité
  - Notions de risque, menace, vulnérabilité
  - Les principes de défense en profondeur, moindre privilège et d'amélioration continu
- Panorama des menaces numériques actuelles
  - Erreur humaine et négligence
  - Phishing et ingénierie sociale
  - Ransomwares et malwares
  - Attaques internes vs externes (Brute force, DDOS, supply chain…)
  - Les tendances actuelles : Cloud, mobilité, IA malveillante
- Culture de sécurité et comportements responsables
  - Sensibilisation aux risques humains et aux vecteurs

d'attaque.
- Importance de l'analyse de risque
- Bonnes pratiques comportementales à mettre en oeuvre : Gestion des mots de passe ; usage des outils collaboratifs et téléchargement, verrouillage de session…
- Notions de traçabilité et de confidentialité
- Posture proactive face aux incidents : Détection et signalement
- Focus sur la protection des données et cadre réglementaire: Typologie des données et principes clés du RGPD

Jour 2

BONNES PRATIQUES DE SÉCURITÉ DU SI

- Bonnes pratiques numériques essentielles
  - Mots de passe et authentification multifactorielle
  - Sécurité des emails et pièces jointes
  - Navigation web et téléchargements
  - Règles d'usage (poste de travail, télétravail, mobilité), usages personnels vs professionnels
  - Supports amovibles et partages de fichiers
  - Sauvegardes
  - Protection des données : Classification de l'information, chiffrement et hébergement
  - Sensibilisation continue des utilisateurs
- Sécurité du poste de travail et de l'environnement
  - Sécurité du poste de travail (Antivirus, EDR/Pare feu...) et de l'environnement (WI Fi, périphériques)
  - Importance des mises à jour et correctifs
  - Sécurité physique (documents, bureau, déplacements)
- Cas des incidents de sécurité
  - Définition d'un incident de sécurité
  - Signaux faibles et alertes
  - Que faire ou ne pas faire en cas d'incident
  - Processus de signalement (Equipe SSI,...)
  - Notions de continuité d'activité
- Gouvernance et organisation SSI
  - Rôles et responsabilités individuelles & collectives (RSSI, équipes IT, métiers)
  - Politiques de sécurité et référentiels : de la PSSI (Politique de Sécurité des SI) aux normes (ISO 27001, NIST, ANSSI)
  - Comprendre la chaîne de décision et les processus de gestion des incidents. (Détection et réaction en cas d'incident)
  - Les mécanismes de détection (SOC) et réaction
  - Importance d'une communication efficace et des circuits d'alerte
- Maintien du socle commun

  - Identifier les composants essentiels : politiques, procédures, outils
  - Assurer la mise à jour et à l'évolution du socle en fonction des menaces
  - Intégrer la sécurité dès la conception ("Security by Design")
  - Réaliser des contrôles réguliers : Audits, Scans de vulnérabilités
- Veille et amélioration continue
  - Mettre en place une veille réglementaire et technologique. Bulletins d'alerte, les différentes sources (CERT, ANSSI, éditeurs…)
  - Analyser les retours d'expérience pour renforcer la culture SSI
  - Définir des indicateurs pour mesurer la maturité de sécurité
- Conclusion
  - Synthèse des deux jours
  - Rappel des messages clés : La sécurité est l'affaire de tous, la logique : prévenir → détecter → réagir…
  - Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com