Les essentiels de la cybersécurité

★★★★★

SII-422 **2 Jours (14 Heures)**

Description

Protéger ses réseaux, ses équipements, documents contre des cyberattaques : chaque jour, de nouveaux exemples illustrent l'importance de la cybersécurité ! Mais au fait, à quels types de risques sommes-nous exposés? Quelle sécurité mettre en place? Nous vous proposons de découvrir la cybersécurité et les différents risques auxquels vous pouvez être exposé!

À qui s'adresse cette formation ?

Pour qui

Toutes les fonctions concernées par la sécurité informatique des organisations, notamment : direction générale, informatique/IT, qualite, management des risques...

Prérequis

Aucun

Les objectifs de la formation

- Identifier les différentes typologies de risques.
- Connaître les référentiels et outils indispensables en matière de cyber sécurité.
- Maîtriser les notions essentielles pour bâtir votre stratégie de défense.

Programme de la formation

Critères de la sécurité

- Fondamentaux : disponibilité, intégrité, confidentialité, traçabilité/ prouvabilité...
- Complémentaires : authenticité, non-répudiation...
- Cybersécurité, Cybercriminalité, Intelligence économique… : les définitions
- Lien avec la politique de cybersécurité

Sécurité des systèmes d'information : quels enjeux

- Menaces, vulnérabilités : état des lieux, veille
- Cybercriminalité : quelle organisation ?
- Ingénierie sociale : notions-clés

Structure du système d'information

- Poste client, applications métiers et transverses, infrastructure d’application, infrastructure (physique, matériel, réseaux)
- Comment établir la cartographie des SI de son entreprise ?
- Focus sur le patrimoine et le système informationnel de votre ordinateur
- Comment construire un réseau de partage de documents sécurisé ?

Les fondamentaux de l’authentification utilisateur

- Méthodes d’identification utilisateur : découverte
- Identifier les bonnes pratiques en matière de mots de passe

Typologie des risques de cybersécurité

- Systémiques (système de management), opérationnels (ISO 27005...), conformité/compliance (ISO 19600…)
- Valeur des biens, biens sensibles et types, impacts internes et externes d’un sinistre (financier, image, réputation, social, économique...)
- Propriétés de sécurité : les grands principes

Référentiels systémiques

- Les bases d’un système (système informatique, système de management, sécurité de l’information vs sécurité du système d’information...)
- Les fondamentaux : ISO 27001, RGPD/ISO 27701 (vie privée), ISO 29100 (cadre privée), ISO 20000-1 (gestion service), ISO 22301 (continuité)...
- Veille normative, légale, réglementaire
- Les acteurs : responsable sécurité de l’information, délégué à la protection des données, responsable système d’information, responsable système de management, responsable conformité…
- Les institutions de référence en matière de cybersécurité : quelles missions ? Qui contacter et dans quel but ?