Comprendre et appliquer le Cyber Resilience Act

Anticiper la cybersécurité des produits numériques dès leur conception

DURÉE
1 jour (7 heures)

EFFECTIF
Jusqu'à 12 personnes

TARIF ADHÉRENT
580 € HT

TARIF NON ADHÉRENT
740 € HT

OBJECTIFS DE LA FORMATION

- Comprendre les enjeux du CRA : renforcer la cybersécurité des produits numériques connectés contre les vulnérabilités et cybermenace
- Comprendre le champ d'application du CRA : Les entreprises concernées, les types de produits, les sanctions en cas de non-respect
- Connaître les exigences essentielles : Sécurité par design, gestion des vulnérabilités, évaluation de conformité, marquage CE
- Savoir appliquer le CRA dans son environnement-métier

PUBLIC VISÉ & PRÉREQUIS

PUBLIC VISÉ
Dirigeants, Responsables R&D/innovation, Chefs de projets, Ingénieurs R&D, Qualiticiens

PRÉREQUIS
Connaissances générales du fonctionnement d'une organisation ou d'un site industriel. Sensibilité aux enjeux énergétiques et climatiques. Aucun prérequis technique approfondi n'est nécessaire.

PROGRAMME DE LA FORMATION

9h - 9h45	**Module 1 : Comprendre le règlement** • Éléments de contexte, enjeux, dates • Impact opérationnel pour les entreprises
9h45 - 10h30	**Module 2 : Cadre d'application** • Le CRA dans le cycle de vie du produit • Responsabilité étendue sur la chaine de valeur (fabricant/importateur/distributeur) • Sanctions encourues • Savoir lire et exploiter le règlement
10h30 - 12h	**Module 3 : Répondre aux attendus règlementaires durant la conception du produit I** • Organiser la démarche de conformité CRA • Classifier les produits, impact sur la méthodologie d'évaluation de la conformité • Connaitre les exigences essentielles de cybersécurité énoncées dans le CRA
12h - 13h30	**Déjeuner**
13h30 - 15h30	**Module 4 : Répondre aux attendus règlementaires durant la conception du produit II** • L'analyse des risques : un document-pilier – Méthode et exemple • Concevoir un produit cyber-resilient : Les points d'attention • La gestion des vulnérabilités : Méthode et outils • Importance de la documentation technique et de la documentation utilisateur
15h30 - 17h30	**Module 5 : Répondre aux attendus règlementaires durant l'exploitation du produit** • Surveillance, gestion continue des vulnérabilités, vulnérabilités activement exploitées • Plan de gestion des incidents • Plan de divulgation des incidents

MOYENS PÉDAGOGIQUES & MODALITÉS D'ÉVALUATION

MOYENS PÉDAGOGIQUES

- Exposés illustrés et séance de questions/réponses directement durant la formation
- Support de cours
- Déjeuner(s) – rencontre pris en commun avec l'intervenant

MODALITÉS D'ÉVALUATION

- Questionnaire préalable à la formation
- Questionnaire d'évaluation et de satisfaction

FORMATEURS & CONTACTS

INTERVENANTS : TEKIN

Expert en conception de solutions IoT et produits numériques sécurisés

CONTACT FORMATIONS

Frédéric CABAS - Responsable Formations
frederic.cabas@polesmartpower.fr
06 12 25 21 26