

Cyber Resilience Act (CRA) : comprendre les exigences et préparer la conformité des produits numériques

Référence : SECCRA

Durée : 2 jours (14 heures)

Certification : Aucune

CONNAISSANCES PRÉALABLE

- Posséder des connaissances générales sur les produits numériques, les logiciels ou les systèmes connectés
- Disposer de notions fondamentales en cybersécurité (vulnérabilités, menaces, risques et mesures de protection)
- Aucune connaissance préalable du Cyber Resilience Act n'est requise

PROFIL DES STAGIAIRES

- Cette formation s'adresse aux professionnels impliqués dans la conception, le développement, la fabrication, la commercialisation ou la conformité de produits comportant des éléments numériques
- Elle concerne notamment les responsables cybersécurité et RSSI, responsables R&D, développeurs logiciels et systèmes embarqués, architectes techniques, responsables qualité et conformité, responsables du marquage CE, chefs de projet produit, Product Owners et responsables techniques

OBJECTIFS

- Expliquer les objectifs, le champ d'application et les principales exigences du Cyber Resilience Act
- Identifier les produits concernés et déterminer les responsabilités des différents opérateurs économiques
- Traduire les exigences de cybersécurité du CRA en mesures applicables à la conception, au développement et à la maintenance des produits
- Réaliser une première analyse des risques de cybersécurité d'un produit numérique
- Organiser la gestion des vulnérabilités et les obligations de notification sur le cycle de vie du produit
- Identifier les procédures d'évaluation de conformité applicables et préparer les principaux éléments du dossier technique
- Construire un plan d'action pour préparer la mise en conformité d'un produit numérique

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'un support pédagogique numérique, d'extraits commentés du règlement CRA, d'une grille de qualification des produits, d'un modèle d'analyse des risques, d'une checklist des exigences essentielles, d'un modèle de processus de gestion des vulnérabilités, d'une trame de dossier technique et d'un modèle de plan d'action
- La formation repose sur une alternance d'apports réglementaires, de présentation d'exemples concrets, d'études de cas et de travaux pratiques. Les exercices sont organisés autour d'un produit numérique fictif utilisé comme fil conducteur sur les deux journées
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

- Consultant-formateur expert en Cybersécurité et notamment du Cyber Resilience Act

MÉTHODES D'ÉVALUATION DES ACQUIS

- Validation des prérequis envoyée en amont de la formation. En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués
- Évaluations formatives : quiz, exercices de classification, analyses de risques, études de cas et productions documentaires. Les travaux font l'objet de corrections et de retours du formateur
- Évaluation finale : mise en situation professionnelle consistant à préparer la conformité CRA d'un produit numérique fictif. Le participant devra qualifier le produit, identifier les obligations applicables, proposer les principales mesures de sécurité, organiser la gestion des vulnérabilités et définir les éléments documentaires et actions nécessaires. Les compétences sont évaluées à l'aide d'une grille alignée sur les objectifs pédagogiques
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

ACCESSIBILITÉ DE LA FORMATION

- Si vous avez besoin d'un aménagement pour suivre votre formation dans de bonnes conditions, nous vous invitons à contacter notre référent handicap au 01 71 19 70 30 ou à l'adresse referent.handicap@edugroupe.com. Un échange en amont nous permettra d'étudier avec vous les adaptations possibles.

CONTENU DU COURS

1. JOUR 1 - Comprendre le CRA et ses exigences de cybersécurité

2. Comprendre les enjeux et le cadre réglementaire du CRA - 1h

- Évolution des cybermenaces affectant les produits numériques et connectés
- Origine et objectifs du règlement européen (UE) 2024/2847
- Principes de sécurité des produits tout au long de leur cycle de vie
- Calendrier d'entrée en application des obligations
- Autorités de surveillance du marché, responsabilités et sanctions
- Articulation générale avec le cadre réglementaire européen de cybersécurité

3. Identifier les produits concernés et les acteurs responsables - 1h30

- Définition des produits comportant des éléments numériques
- Produits matériels, logiciels, systèmes embarqués, objets connectés et solutions de traitement à distance associées
- Produits et situations exclus ou soumis à des dispositions particulières
- Classification des produits : catégories par défaut, produits importants de classes I et II, produits critiques
- Rôles et obligations des fabricants, importateurs, distributeurs et mandataires
- Responsabilités en cas de modification substantielle ou de commercialisation sous sa propre marque
- Cas particuliers des composants logiciels et des logiciels libres et open source
- 💡 *Atelier pratique : analyser un portefeuille de produits numériques et déterminer leur champ d'application, leur catégorie et les responsabilités associées*

4. Intégrer les exigences essentielles de cybersécurité - 2h

- Présentation des exigences essentielles de l'annexe I du CRA
- Principes de Security by Design et Security by Default
- Sécurisation des configurations et des paramètres par défaut
- Gestion des identités, authentification et contrôle des accès
- Protection des données, confidentialité et intégrité
- Réduction de la surface d'attaque et protection contre les accès non autorisés
- Disponibilité, résilience et limitation des impacts des incidents
- Journalisation et capacités de surveillance
- Mises à jour de sécurité et mécanismes de correction
- Intégration de la cybersécurité dans les processus de développement et de maintenance
- 💡 *Atelier pratique : identifier les mesures de sécurité à prévoir pour un produit connecté et construire une grille de vérification des exigences essentielles*

5. Comprendre les procédures d'évaluation de conformité - 1h15

- Principes de l'évaluation de conformité
- Différences entre les procédures d'autoévaluation et celles impliquant un organisme notifié
- Incidence de la catégorie du produit sur les procédures applicables
- Rôle des normes harmonisées et des spécifications communes
- Place des référentiels techniques et des certifications de cybersécurité
- Préparation des preuves nécessaires à la démonstration de conformité
- 💡 *Étude de cas : déterminer les démarches d'évaluation de conformité envisageables pour plusieurs catégories de produits*

6. Articuler le CRA avec les autres réglementations et référentiels - 1h15

- Relations entre le CRA et la directive NIS2
- Articulation avec le RGPD pour les produits traitant des données personnelles
- Interactions avec la directive RED et le règlement Machines
- Complémentarités avec l'AI Act pour les produits intégrant des fonctionnalités d'IA
- Apports des référentiels IEC 62443, ISO/IEC 27001 et ISO/IEC 27005
- Identification des exigences communes et des obligations spécifiques
- 💡 *Atelier pratique : construire une matrice simplifiée des exigences réglementaires et normatives applicables à un produit numérique*

7. JOUR 2 - Construire une démarche de conformité CRA

8. Réaliser une analyse des risques de cybersécurité produit - 2h

- Principes de l'analyse des risques exigée par le CRA
- Identification des fonctions essentielles, des actifs et des interfaces du produit
- Analyse des menaces, des vulnérabilités et des scénarios d'attaque
- Évaluation des impacts et des niveaux de risques
- Définition et justification des mesures de traitement
- Prise en compte des risques liés aux composants tiers et à la chaîne d'approvisionnement logicielle
- Présentation des approches ISO/IEC 27005, EBIOS Risk Manager et IEC 62443
- Documentation et actualisation de l'analyse des risques
- 💡 *Atelier pratique : réaliser une analyse des risques simplifiée sur un produit connecté et proposer les mesures de sécurité adaptées*

9. Organiser la gestion des vulnérabilités et des incidents - 2h

- Obligations de gestion des vulnérabilités pendant la période de support
- Identification, qualification et priorisation des vulnérabilités
- Gestion des composants logiciels tiers et Software Bill of Materials (SBOM)
- Utilisation des références CVE et des scores CVSS
- Processus de correction, tests et diffusion des mises à jour
- Divulgaration coordonnée des vulnérabilités
- Obligations de notification des vulnérabilités activement exploitées et des incidents graves ayant un impact sur la sécurité du produit
- Délais et modalités de notification auprès des autorités compétentes
- Information des utilisateurs et organisation du support de sécurité
- 💡 *Atelier pratique : définir un processus de traitement d'une vulnérabilité critique, depuis sa détection jusqu'à la correction et aux éventuelles notifications réglementaires*

10. Préparer le dossier technique et la conformité CE - 1h45

- Objectifs et contenu du dossier technique de conformité
- Description du produit, de ses fonctions et de son architecture
- Documentation de l'analyse des risques et des mesures de sécurité
- Justification du respect des exigences essentielles
- Rapports d'essais, contrôles et éléments de preuve
- Documentation des procédures de gestion des vulnérabilités et de mise à jour
- Préparation de la déclaration UE de conformité
- Principes et conditions du marquage CE
- Conservation des documents, traçabilité et obligations après commercialisation
- Préparation aux demandes des autorités de surveillance du marché
- 💡 *Atelier pratique : construire la structure d'un dossier technique CRA et identifier les documents et preuves à réunir*

11. Construire une feuille de route de mise en conformité - 1h15

- Réaliser un diagnostic initial de conformité
- Identifier les écarts entre les pratiques existantes et les exigences applicables
- Définir les responsabilités entre R&D, cybersécurité, qualité, conformité et direction
- Prioriser les actions de remédiation
- Intégrer les exigences CRA dans les processus de développement, d'achat et de gestion des fournisseurs
- Définir les jalons, ressources et indicateurs de suivi
- Organiser la veille réglementaire et l'amélioration continue
- 💡 *Atelier final : élaborer une feuille de route de conformité CRA pour un produit numérique, comprenant les écarts identifiés, les actions prioritaires, les responsables, les échéances et les preuves attendues*