PRESENTATION DU CYBER RESILIENCE ACT (CRA)

Le paysage réglementaire européen connaît une transformation majeure avec l'adoption du Cyber Resilience Act (CRA). Ce règlement est entré en vigueur en décembre 2024 et représente une étape décisive dans la sécurisation des produits numériques commercialisés dans l'Union européenne. Pour les fabricants de machines, d'équipements industriels et de produits connectés, cette réglementation introduit des obligations inédites qui transforment profondément les pratiques de conception et de commercialisation.

Qu'est-ce que le CRA ?

Le Cyber Resilience Act (Règlement UE 2024/2847) est un règlement européen d'application directe qui établit des exigences harmonisées de cybersécurité pour tous les « produits comportant des éléments numériques » mis à disposition sur le marché de l'Union européenne. Contrairement aux directives qui nécessitent une transposition nationale, le CRA s'applique de manière uniforme dans l'ensemble des États membres dès son entrée en vigueur.

Un règlement d'application directe

Le caractère directement applicable du CRA signifie qu'aucune transposition nationale n'est nécessaire. Les fabricants, qu'ils soient établis dans l'UE ou dans des pays tiers, doivent se conformer aux mêmes exigences pour commercialiser leurs produits sur le marché européen. Cette uniformisation vise à créer un niveau de sécurité homogène et à éviter la fragmentation réglementaire.

Périmètre d'application

Le CRA s'applique à tout produit comportant des éléments numériques, c'est-à-dire tout matériel ou logiciel capable de traiter des données numériques. Cela inclut notamment :

- Les produits de grande consommation (smartphones, ordinateurs portables, objets connectés, domotique)
- Les équipements industriels connectés (machines, robots, automates)
- Les systèmes de contrôle-commande (PLC, SCADA, DCS)
- Les dispositifs IoT et IIoT
- Les logiciels embarqués et firmware
- Les composants de cybersécurité eux-mêmes

Le règlement couvre l'ensemble du cycle de vie du produit, de sa conception jusqu'à sa mise hors service, en passant par sa distribution et son utilisation.

Quels sont les objectifs du CRA ?

Le Cyber Resilience Act poursuit plusieurs objectifs stratégiques qui reflètent les enjeux de cybersécurité actuels dans un contexte d'interconnexion croissante des systèmes industriels et grand public.

Renforcer la sécurité by design

L'objectif central du CRA est d'imposer une approche « security by design » (sécurité dès la conception) pour tous les produits numériques. Cette philosophie exige que la cybersécurité soit intégrée dès les premières phases de développement, et non ajoutée comme une couche supplémentaire après coup. Les fabricants doivent anticiper les menaces, évaluer les risques et implémenter des mécanismes de protection adaptés avant même la mise sur le marché.

Améliorer la transparence et la confiance

Le CRA vise à créer un environnement de confiance en imposant aux fabricants de communiquer clairement sur les caractéristiques de sécurité de leurs produits. Les utilisateurs et intégrateurs doivent pouvoir

identifier facilement les produits conformes grâce au marquage CE et disposer d'informations détaillées sur les mesures de sécurité implémentées, les vulnérabilités connues et les mises à jour disponibles.

Créer une chaîne de responsabilité

En responsabilisant l'ensemble des acteurs économiques (fabricants, importateurs, distributeurs), le règlement établit une chaîne de responsabilité claire. Chaque intervenant doit s'assurer que les produits qu'il met à disposition respectent les exigences du CRA, créant ainsi un écosystème où la cybersécurité devient une préoccupation partagée.

Harmoniser les exigences au niveau européen

L'harmonisation réglementaire évite la multiplication de normes nationales divergentes qui compliqueraient la commercialisation transfrontalière. Un produit conforme au CRA peut être librement commercialisé dans l'ensemble de l'Union européenne, simplifiant les démarches pour les fabricants tout en garantissant un niveau de protection uniforme pour les utilisateurs.

Qu'est-ce qui change avec le CRA ?

L'entrée en vigueur du Cyber Resilience Act marque un changement de paradigme pour l'industrie manufacturière et les éditeurs de logiciels. Les obligations imposées transforment profondément les pratiques établies.

Une approche réglementaire contraignante

Contrairement aux recommandations et bonnes pratiques volontaires qui prévalaient jusqu'alors, le CRA impose des obligations juridiquement contraignantes. Les fabricants ne peuvent plus choisir d'ignorer la cybersécurité : elle devient une condition légale pour accéder au marché européen, au même titre que la sécurité fonctionnelle ou la compatibilité électromagnétique.

La gestion proactive des vulnérabilités

L'une des innovations majeures du CRA concerne la gestion des vulnérabilités. Le règlement distingue deux types de vulnérabilités nécessitant une réaction rapide :

- **Les vulnérabilités activement exploitées** : lorsqu'un fabricant découvre qu'une vulnérabilité dans son produit fait l'objet d'une exploitation malveillante en conditions réelles, il dispose de 24 heures pour effectuer une notification initiale, 72 heures pour fournir des premières mesures correctives, et 14 jours pour soumettre un rapport final.
- **Les vulnérabilités exploitables** : ces failles présentent un potentiel d'exploitation dans des conditions opérationnelles pratiques. Bien que le CRA n'impose pas de délais stricts pour leur traitement, elles ne doivent plus être présentes dans les produits commercialisés après la date d'application complète du règlement.

L'obligation de support sur la durée

Le CRA impose aux fabricants de fournir des mises à jour de sécurité pendant une période minimale de 5 ans après la mise sur le marché. Cette obligation transforme le modèle économique de nombreux fabricants habitués à une logique de vente unique, en les contraignant à maintenir une relation continue avec leurs produits et leurs clients.

La traçabilité et la documentation

Les exigences documentaires deviennent considérablement plus importantes. Les fabricants doivent constituer et maintenir une documentation technique détaillée comprenant notamment :

- L'analyse de risques cybersécurité
- La description des fonctionnalités de sécurité
- Les résultats des tests et évaluations
- Le processus de gestion des vulnérabilités
- Les instructions d'installation et d'utilisation sécurisées

Cette documentation doit être conservée pendant 10 ans et mise à disposition des autorités de surveillance sur demande.

Qui est concerné par le CRA ?

Le périmètre d'application du Cyber Resilience Act est volontairement large pour couvrir l'ensemble des acteurs économiques impliqués dans la mise à disposition de produits numériques.

Les fabricants

Les fabricants constituent la catégorie d'acteurs la plus directement concernée. Sont considérés comme fabricants :

- Les entreprises qui conçoivent et produisent des produits avec éléments numériques
- Les entreprises qui font concevoir ou fabriquer de tels produits et les commercialisent sous leur nom ou marque
- Les importateurs qui introduisent sur le marché européen des produits de fabricants établis hors UE
- Les distributeurs qui deviennent responsables lorsqu'ils modifient substantiellement un produit ou le mettent à disposition alors qu'il n'est manifestement pas conforme

Cette définition large englobe aussi bien les grands groupes industriels que les PME et startups développant des solutions connectées.

Les secteurs industriels particulièrement impactés

Plusieurs secteurs sont particulièrement concernés par le CRA :

L'industrie manufacturière : Les constructeurs de machines-outils, d'équipements de production, de robots industriels et d'automates programmables sont en première ligne. Leurs produits, de plus en plus connectés et intégrés dans des architectures IIoT, entrent pleinement dans le champ d'application du règlement.

L'automatisation industrielle : Les fabricants de systèmes de contrôle-commande (SCADA, DCS, PLC), de capteurs intelligents et d'interfaces homme-machine (HMI) doivent adapter leurs processus de développement pour répondre aux exigences du CRA.

L'IoT et l'électronique grand public : Les produits connectés destinés aux particuliers (objets connectés, équipements domotiques, dispositifs de surveillance) sont également soumis au règlement.

Les éditeurs de logiciels : Les développeurs de systèmes d'exploitation, de firmware, d'applications industrielles et de solutions de cybersécurité elles-mêmes doivent se conformer au CRA.

Classification des produits

Le CRA établit une classification des produits en fonction de leur criticité, avec des exigences et procédures d'évaluation différenciées :

Produits standards : La majorité des produits avec éléments numériques relèvent de cette catégorie. Ils font l'objet d'une auto-évaluation de conformité par le fabricant (Module A), qui peut s'appuyer sur des normes harmonisées une fois qu'elles seront publiées.

Produits de Classe I (Important) : Cette catégorie regroupe certains produits de gestion d'identité, de contrôle d'accès, de réseaux privés virtuels et de systèmes détectant des vulnérabilités. Ils nécessitent une auto-évaluation avec respect de normes harmonisées lorsqu'elles existent.

Produits de Classe II (Important) : Incluent notamment les systèmes d'exploitation, les microprocesseurs sécurisés et certains systèmes de détection d'intrusion. Ils requièrent un examen de type par un organisme notifié (Module B+C).

Produits Critiques : Les produits les plus sensibles (par exemple, certains composants de sécurité pour infrastructures critiques) peuvent être soumis à un schéma européen de certification cybersécurité.

Les acteurs indirectement concernés

Au-delà des fabricants, d'autres parties prenantes sont impactées :

- **Les intégrateurs de systèmes** qui assemblent des produits numériques dans des installations complexes doivent s'assurer de la conformité des composants utilisés
- **Les opérateurs industriels** ont intérêt à exiger la conformité CRA de leurs fournisseurs pour sécuriser leurs installations

- **Les sous-traitants et fournisseurs** intervenant dans la chaîne de développement doivent adapter leurs pratiques pour permettre la conformité du produit final

Quelles sont les obligations principales pour les organisations industrielles ?

Le CRA impose un ensemble d'obligations qui structurent l'approche cybersécurité tout au long du cycle de vie du produit. Ces exigences se déclinent en plusieurs catégories complémentaires.

Exigences essentielles de cybersécurité

Les exigences essentielles définies à l'Annexe I du CRA constituent le socle de sécurité que tout produit doit respecter. Elles incluent notamment :

Sécurité dès la conception : Les produits doivent être conçus, développés et produits de manière à garantir un niveau approprié de cybersécurité basé sur les risques. Cela implique une analyse de risques formalisée, l'identification des actifs critiques et menaces potentielles, et la mise en œuvre de mesures de protection proportionnées.

Défense en profondeur : Le règlement encourage l'adoption d'architectures de sécurité multicouches, où plusieurs mécanismes de protection se renforcent mutuellement. Cette approche, bien connue dans les environnements OT sous le principe de "defense in depth", limite l'impact d'une compromission ponctuelle.

Réduction de la surface d'attaque : Les fabricants doivent minimiser les fonctionnalités inutiles, désactiver les services non essentiels et limiter les privilèges d'accès au strict nécessaire. Les composants logiciels et matériels doivent être choisis en privilégiant ceux présentant le moins de vulnérabilités connues.

Gestion des mises à jour : Les produits doivent pouvoir recevoir des mises à jour de sécurité tout au long de leur période de support. Ces mises à jour doivent être sécurisées (signées, authentifiées), faciles à appliquer et ne pas dégrader les fonctionnalités du produit.

Gestion des vulnérabilités

La gestion des vulnérabilités constitue l'une des obligations les plus exigeantes du CRA. Les fabricants doivent établir et maintenir un processus complet comprenant :

Identification et réception : Mise en place d'un point de contact unique pour recevoir les signalements de vulnérabilités (security.txt conformément à la RFC 9116). Les fabricants doivent surveiller activement les bases de données de vulnérabilités (CVE, NVD) concernant les composants qu'ils intègrent.

Analyse et évaluation : Chaque vulnérabilité doit être analysée pour déterminer son exploitabilité dans le contexte spécifique du produit. Cette évaluation doit considérer l'environnement d'utilisation prévu, les mesures de protection existantes et les conditions pratiques d'exploitation. Une vulnérabilité théorique dans un composant peut ne pas être exploitable si ce composant est isolé du réseau ou protégé par d'autres mécanismes.

Traitement et remédiation : En fonction de la criticité et de l'exploitabilité, le fabricant doit développer et déployer des correctifs, des contournements ou des mesures compensatoires. Le règlement reconnaît la notion de "patching virtuel" (virtual patching), particulièrement pertinente pour les environnements OT où les mises à jour logicielles peuvent être difficiles à appliquer.

Communication : Les fabricants doivent communiquer de manière transparente sur les vulnérabilités et les mesures correctives. Cette communication doit être à la fois proactive (notifications aux utilisateurs) et réactive (réponses aux demandes d'information).

Documentation technique

La constitution d'une documentation technique complète et maintenue à jour est obligatoire. Cette documentation doit inclure :

- Une déclaration de conformité UE attestant le respect des exigences essentielles

- La documentation de l'analyse de risques cybersécurité
- La description détaillée des propriétés de sécurité du produit
- Les instructions pour une installation, configuration et utilisation sécurisées
- La politique de gestion des vulnérabilités et des mises à jour
- Les résultats des tests et évaluations de sécurité effectués

Marquage CE et déclaration de conformité

Avant de commercialiser un produit, le fabricant doit :

- Réaliser l'évaluation de conformité selon la procédure applicable (Module A, A avec norme harmonisée, ou B+C selon la classe)
- Établir la déclaration de conformité UE
- Apposer le marquage CE sur le produit
- Fournir les instructions et informations de sécurité nécessaires

Obligations de support et de maintenance

Les obligations principales ne prendront pleinement effet qu'au 11 décembre 2027, mais les fabricants doivent dès maintenant planifier leur stratégie de support sur le long terme. L'obligation de fournir des mises à jour de sécurité pendant au moins 5 ans transforme le modèle de relation client et nécessite une organisation dédiée pour le support post-vente.

Quelles sont les sanctions prévues par le CRA ?

Le Cyber Resilience Act prévoit un régime de sanctions dissuasif pour garantir l'effectivité des obligations imposées. Les autorités nationales de surveillance disposent de pouvoirs d'investigation, d'injonction et de sanction étendus.

Sanctions financières

Les amendes peuvent atteindre 15 millions d'euros ou 2,5% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Cette double approche permet d'adapter la sanction à la taille de l'entreprise : les grandes organisations encourent des amendes proportionnelles à leur chiffre d'affaires, tandis qu'un plancher de 15 millions d'euros garantit le caractère dissuasif même pour des entreprises de taille plus modeste.

La proportionnalité des sanctions dépend de plusieurs critères :

- La nature, la gravité et la durée du manquement
- Le caractère intentionnel ou négligent de l'infraction
- Les mesures prises pour atténuer les dommages
- Le degré de coopération avec les autorités
- Les manquements antérieurs éventuels
- Les conséquences du manquement sur les utilisateurs et la société

Sanctions administratives

Au-delà des amendes financières, les autorités de surveillance peuvent prendre diverses mesures :

Injonctions : Obligation de mettre en conformité le produit dans un délai déterminé, de fournir des informations complémentaires, ou de corriger des pratiques non conformes.

Retrait et rappel : En cas de manquement grave, l'autorité peut exiger le retrait du produit du marché et son rappel auprès des utilisateurs finaux. Cette mesure, particulièrement coûteuse et dommageable pour l'image de l'entreprise, constitue une sanction dissuasive majeure.

Interdiction de mise sur le marché : Les produits non conformes peuvent se voir interdire l'accès au marché européen jusqu'à ce que leur conformité soit démontrée.

Publication des sanctions : Les autorités peuvent rendre publiques les sanctions prononcées, avec un

impact réputationnel significatif pour les entreprises concernées.

Responsabilité civile et commerciale

Au-delà des sanctions administratives, les fabricants s'exposent également à :

- Des actions en responsabilité civile de la part d'utilisateurs ayant subi un préjudice
- Une perte de confiance et d'image de marque
- L'exclusion de marchés publics ou de certifications sectorielles
- Des difficultés commerciales avec des clients exigeant la conformité

Comment se préparer à l'application du CRA ?

La préparation à la conformité CRA nécessite une approche méthodique et progressive. Bien que les obligations principales s'appliquent à partir du 11 décembre 2027, il est essentiel de commencer dès maintenant, compte tenu de l'ampleur des transformations à opérer.

Étape 1 : Évaluation de l'état des lieux

La première étape consiste à réaliser un diagnostic précis de la situation actuelle :

Inventaire des produits : Identifier tous les produits comportant des éléments numériques commercialisés ou en développement. Pour chaque produit, déterminer sa classification potentielle (standard, classe I, classe II, critique).

Analyse des écarts : Comparer les pratiques actuelles avec les exigences du CRA. Identifier les processus existants (développement sécurisé, gestion des vulnérabilités, support) et les lacunes à combler.

Évaluation des impacts : Estimer les ressources nécessaires (humaines, techniques, financières) pour atteindre la conformité, ainsi que les délais réalistes pour la mise en œuvre.

Étape 2 : Mise en place du management des risques cybersécurité

Le management des risques constitue le fondement de la démarche de conformité. Il s'agit d'adopter une approche structurée, idéalement basée sur des référentiels reconnus comme la norme IEC 62443-4-1 pour le développement de produits sécurisés :

Définir le système considéré : Délimiter précisément le périmètre d'analyse (composants matériels, logiciels, interfaces, environnement d'utilisation prévu).

Identifier les actifs et interfaces : Lister tous les éléments du système susceptibles d'être ciblés par une attaque (données, fonctions critiques, composants de communication).

Analyser les impacts : Évaluer la criticité de chaque actif en termes de confidentialité, intégrité, disponibilité et safety.

Identifier les menaces : Utiliser des méthodologies structurées (STRIDE de Microsoft, MITRE ATT&CK pour ICS) pour recenser les menaces pertinentes selon le contexte d'utilisation.

Évaluer la vraisemblance : Déterminer la probabilité de réalisation de chaque menace en fonction de la motivation des attaquants, des opportunités d'attaque et des mesures de protection existantes.

Calculer et hiérarchiser les risques : Croiser l'impact et la vraisemblance pour obtenir un niveau de risque, puis prioriser les risques à traiter.

Définir et implémenter les mesures de réduction : Sélectionner les mesures techniques et organisationnelles appropriées pour ramener les risques à un niveau acceptable.

Évaluer le risque résiduel : Vérifier que les risques subsistant après traitement sont acceptables au regard du contexte d'utilisation.

Étape 3 : Intégration de la sécurité dans le cycle de développement

La sécurité doit être intégrée à chaque phase du cycle de vie du produit, selon une approche "Secure Development Lifecycle" (SDL) :

Conception : Définir les exigences de sécurité, concevoir l'architecture sécurisée, sélectionner les composants en tenant compte de leur sécurité.

Développement : Appliquer les pratiques de codage sécurisé, utiliser des outils d'analyse statique et dynamique, réaliser des revues de code orientées sécurité.

Tests et validation : Effectuer des tests de sécurité (tests d'intrusion, fuzzing), vérifier la résistance aux attaques identifiées dans l'analyse de risques.

Mise sur le marché : Constituer la documentation technique, réaliser l'évaluation de conformité, établir la déclaration UE de conformité.

Support et maintenance : Surveiller les vulnérabilités, développer et déployer les correctifs, communiquer avec les utilisateurs.

Fin de vie : Informer les utilisateurs de la fin du support de sécurité, fournir des recommandations pour la migration ou le retrait sécurisé.

Étape 4 : Mise en place du processus de gestion des vulnérabilités

Un processus robuste de gestion des vulnérabilités est indispensable :

Création d'un point de contact : Publier un fichier security.txt (RFC 9116) à la racine du site web de l'entreprise, indiquant comment signaler des vulnérabilités de manière responsable.

Veille sur les vulnérabilités : Surveiller les bases CVE/NVD pour les composants tiers utilisés, suivre les avis de sécurité des fournisseurs, participer à des communautés d'échange sur les menaces (ISAC).

Analyse contextuelle : Pour chaque vulnérabilité identifiée, évaluer son exploitabilité réelle dans le contexte spécifique du produit. Une vulnérabilité affectant un composant non exposé ou protégé par des mesures compensatoires peut ne pas nécessiter de correctif urgent.

Développement de correctifs : Prioriser le développement des correctifs selon la criticité et l'exploitabilité, tester les correctifs pour éviter les régressions, préparer les documents VEX (Vulnerability Exploitability eXchange) précisant le statut de chaque vulnérabilité.

Déploiement et communication : Notifier les clients de la disponibilité des correctifs, fournir des instructions claires pour leur application, proposer des mesures de contournement si nécessaire.

Conformité aux délais CRA : Mettre en place des procédures d'urgence pour respecter les délais stricts imposés pour les vulnérabilités activement exploitées (notification initiale sous 24h, rapport complet sous 14 jours).

Étape 5 : Organisation et compétences

La conformité CRA nécessite des compétences spécifiques et une organisation adaptée :

Désigner un responsable produit sécurité : Identifier un porteur du sujet au niveau de la direction, disposant de l'autorité et des ressources nécessaires.

Former les équipes : Sensibiliser l'ensemble des équipes de développement, former aux pratiques de développement sécurisé, développer l'expertise en analyse de risques et gestion des vulnérabilités.

Créer ou renforcer le PSIRT : Mettre en place un Product Security Incident Response Team (PSIRT) chargé de la gestion des vulnérabilités et des incidents de sécurité.

Structurer la gouvernance : Définir les rôles et responsabilités, établir les processus de décision, mettre en place des indicateurs de suivi de la conformité.

Étape 6 : Collaboration avec l'écosystème

La conformité ne peut s'obtenir de manière isolée :

Exigences vis-à-vis des fournisseurs : Intégrer des clauses de sécurité dans les contrats avec les fournisseurs de composants, exiger la fourniture

d'informations sur les vulnérabilités et les correctifs (SBOM, VEX).

Communication avec les clients : Fournir des documentations de sécurité complètes, accompagner les intégrateurs dans le déploiement sécurisé, établir des canaux de communication pour les questions de sécurité.

Participation aux initiatives sectorielles : Rejoindre des groupes de travail professionnels (VDMA, autres associations industrielles), participer aux travaux de normalisation, échanger les bonnes pratiques.

Checklist opérationnelle OT/IoT : 10 actions clés

Pour structurer votre démarche de conformité, voici une checklist pragmatique des actions prioritaires à mettre en œuvre :

1. Réaliser l'inventaire exhaustif des produits concernés

Identifiez tous vos produits comportant des éléments numériques destinés au marché européen. Pour chacun, documentez les composants matériels et logiciels, les interfaces de communication, les versions de firmware, et déterminez la classification CRA applicable.

2. Effectuer l'analyse de risques cybersécurité produit par produit

Appliquez une méthodologie structurée (IEC 62443-4-1, ISO/SAE 21434 pour les produits connectés au véhicule) pour identifier les actifs critiques, les menaces pertinentes, évaluer les risques et définir les mesures de protection adaptées. Documentez formellement cette analyse.

3. Implémenter la défense en profondeur et la segmentation

Adoptez une architecture de sécurité multicouches : segmentation réseau pour isoler les zones critiques, firewalls et IPS pour contrôler les flux, contrôle d'accès stricte, authentification forte. Cette approche réduit considérablement la surface d'attaque et l'exploitabilité des vulnérabilités.

4. Déployer des solutions de cybersécurité OT natives

Les environnements OT nécessitent des solutions spécifiques, différentes des outils IT classiques. Privilégiez :

- Des solutions de protection des endpoints adaptées aux systèmes industriels (support des OS legacy, pas de reboot requis, whitelisting OT)
- Des IPS avec inspection approfondie des protocoles industriels (DPI sur Modbus, Profinet, EtherNet/IP, etc.)
- Des solutions de patching virtuel pour protéger les systèmes non patchables
- Des outils de contrôle des supports amovibles (USB) adaptés aux environnements de production

5. Établir le processus de gestion des vulnérabilités

Mettez en place l'infrastructure nécessaire : point de contact sécurisé (security.txt), veille automatisée sur les CVE, processus d'analyse et de priorisation, capacité de développement et déploiement de correctifs en urgence, communication structurée avec les clients.

6. Mettre en place un système de mise à jour sécurisé

Concevez un mécanisme permettant de déployer des mises à jour de sécurité de manière sécurisée (signature cryptographique, canal authentifié), simple (automatisation possible) et sans interruption prolongée de la production. Prévoyez des mécanismes de rollback en cas de problème.

7. Constituer la documentation technique de conformité

Rassemblez et formalisez l'ensemble de la documentation requise : analyse de risques, spécifications de sécurité, résultats de tests, procédures de configuration sécurisée, politique de gestion des vulnérabilités, manuel d'utilisation

sécurisée. Cette documentation doit être maintenue à jour tout au long du cycle de vie.

8. Définir les conditions d'utilisation sécurisée et les responsabilités

Précisez dans la documentation produit le contexte d'utilisation prévu, les hypothèses de sécurité (environnement réseau, contrôles d'accès physique attendus), les limites de responsabilité. Certaines mesures de sécurité relèvent de l'opérateur final : clarifiez ces responsabilités contractuellement.

9. Former et structurer les équipes

Investissez dans la montée en compétences : formation au développement sécurisé, certification en cybersécurité industrielle (ISA/IEC 62443 Cybersecurity Expert), recrutement de profils spécialisés si nécessaire. Structurez l'organisation avec des rôles dédiés (product security officer, PSIRT).

10. Anticiper le support long terme

Planifiez dès la conception la stratégie de support sur 5 ans minimum : architecture permettant les mises à jour, provisionnement des ressources humaines et techniques pour le support post-vente, modèle économique incluant le coût du support de sécurité. Anticipez la gestion de l'obsolescence des composants.

Comment AKENATECH vous accompagne ?

Face à la complexité et l'ampleur des exigences du Cyber Resilience Act, nous avons développé une approche d'accompagnement complète qui couvre l'ensemble de votre parcours de conformité.

Une expertise reconnue en cybersécurité OT et conformité réglementaire

Notre positionnement unique combine une expertise technique approfondie en cybersécurité des environnements industriels (OT/IoT) avec une maîtrise des enjeux de conformité réglementaire. Nous connaissons les spécificités des systèmes de contrôle-commande, les contraintes de disponibilité des environnements de production, et les exigences des référentiels IEC 62443 et ISO 27001 qui constituent le socle technique de la conformité CRA.

Un accompagnement de bout en bout : Stratégie → Implémentation → Opérations

Notre approche structurée en trois phases assure une transformation durable et efficace :

Phase Stratégie - Conseil en GRC

Nous commençons par une analyse approfondie de votre situation :

- Diagnostic de conformité CRA : identification des produits concernés, évaluation des écarts avec les exigences
- Définition de la stratégie de mise en conformité : priorisation des actions, planification des ressources, estimation des coûts
- Mise en place du management des risques cybersécurité selon IEC 62443-4-1 : méthodologie d'analyse de risques produit, accompagnement sur vos premiers produits pilotes
- Support à la préparation de la documentation technique et des procédures d'évaluation de conformité
- Accompagnement au marquage CE pour les produits avec éléments numériques

Cette phase de conseil permet de construire une feuille de route claire et réaliste, alignée sur vos contraintes métier et vos objectifs commerciaux.

Phase Implémentation - Intégration de solutions

Une fois la stratégie définie, nous passons à la mise en œuvre concrète :

- **Protection des endpoints** : déploiement de solutions de cybersécurité natives pour OT, adaptées aux systèmes industriels et legacy (support Windows 2000/XP et Linux, pas de

reboot nécessaire, whitelisting automatique des applications OT)

- **Visibilité et détection** : mise en place de solutions de monitoring réseau avec inspection approfondie des protocoles industriels (DPI sur 200+ protocoles OT), détection d'anomalies et d'intrusions
- **Durcissement des systèmes** : application des bonnes pratiques de configuration sécurisée, désactivation des services inutiles, contrôle d'accès renforcé
- **Scellement et intégrité** : solutions de protection contre la modification non autorisée, contrôle des supports amovibles (USB) adapté aux environnements de production
- **Segmentation et défense en profondeur** : architecture réseau sécurisée avec IPS/IDS, firewalls industriels, isolation des zones critiques

Nous privilégions des solutions éprouvées dans les environnements OT, avec des partenaires technologiques reconnus comme TXOne Networks, qui proposent notamment des mécanismes de patching virtuel particulièrement adaptés aux contraintes du CRA.

Phase Opérations - Services managés

La conformité CRA n'est pas un projet ponctuel mais un engagement sur la durée. Nous assurons la continuité de votre conformité :

- **RSSI à temps partagé** : mise à disposition d'un Responsable de la Sécurité des Systèmes d'Information expérimenté pour piloter votre démarche de sécurité produit sans recruter en interne
- **PSIRT semi-externalisé** : gestion opérationnelle de vos vulnérabilités, veille CVE automatisée, analyse d'exploitabilité, coordination du développement et déploiement des correctifs, communication avec les clients et autorités
- Support continu pour l'évolution de votre documentation et de vos processus

Une approche pragmatique et opérationnelle

Notre méthodologie est conçue pour être pragmatique et adaptée aux réalités industrielles :

- Prise en compte des contraintes de production (disponibilité, legacy, environnements air-gapped)
- Approche progressive et par priorité pour maîtriser les investissements
- Transfert de compétences pour autonomiser vos équipes
- Réutilisation des analyses et investissements existants (ISO 27001, NIS2, IEC 62443)

Synergie avec les autres réglementations

Le CRA ne s'applique pas de manière isolée. Nous vous aidons à créer des synergies avec vos autres démarches de conformité :

- **Règlement Machines 2023/1230** : coordination des exigences de cybersécurité communes avec le CRA
- **NIS2** : alignement des mesures organisationnelles et techniques pour les opérateurs critiques
- **ISO 27001** : intégration de la sécurité produit dans votre système de management de la sécurité de l'information
- **IEC 62443** : référentiel technique de référence pour la cybersécurité industrielle, reconnu comme base solide pour la conformité CRA

FAQ

Quand le CRA entre-t-il réellement en application ?

Le Cyber Resilience Act est entré en vigueur le 10 décembre 2024. Cependant, les obligations s'appliquent progressivement :

- **11 septembre 2026** : obligation de signalement des vulnérabilités activement exploitées et des incidents de sécurité graves
- **11 décembre 2027** : application complète de toutes les exigences, y compris l'interdiction de commercialiser des produits avec des vulnérabilités exploitables connues

Il est donc crucial de commencer votre démarche dès maintenant, car les transformations nécessaires demandent du temps.

Mon produit est-il concerné par le CRA ?

Si votre produit comporte des éléments numériques (matériel ou logiciel capable de traiter des données numériques) et qu'il est destiné à être commercialisé dans l'Union européenne, il est très probablement concerné. Cela inclut notamment :

- Les produits de consommations incorporant des éléments numériques
- Les machines industrielles avec automates programmables
- Les équipements connectés (IoT/IIoT)
- Les systèmes de contrôle-commande (SCADA, DCS, PLC)
- Les composants électroniques avec firmware
- Les logiciels embarqués et applications industrielles

Certaines exemptions existent (dispositifs médicaux, véhicules, aéronautique déjà couverts par d'autres réglementations spécifiques), mais elles sont limitées.

Quelle est la différence entre le CRA et le Règlement Machines ?

Le **Règlement Machines (EU) 2023/1230** s'applique spécifiquement aux machines et établit des exigences de sécurité fonctionnelle (safety) incluant désormais des aspects de cybersécurité. Le **CRA** s'applique de manière horizontale à tous les produits avec éléments numériques, qu'ils soient ou non des machines.

Pour un fabricant de machines, les deux réglementations s'appliquent de manière complémentaire :

- Le Règlement Machines couvre la sécurité fonctionnelle globale de la machine (risques mécaniques, électriques, cybersécurité affectant la sécurité)
- Le CRA couvre tous les aspects de cybersécurité des éléments numériques de la machine

Les exigences se recoupent partiellement, et une analyse de risques bien menée permet de répondre simultanément aux deux réglementations.

Dois-je traiter toutes les vulnérabilités CVE affectant mes composants ?

Non, l'approche du CRA est basée sur le risque et l'exploitabilité en conditions réelles. Une vulnérabilité CVE affectant un composant que vous utilisez n'est pas nécessairement exploitable dans votre produit, en fonction :

- De votre architecture de sécurité (segmentation, défense en profondeur)
- Du contexte d'utilisation (composant non exposé au réseau, accès physique requis pour l'exploitation)
- Des fonctionnalités effectivement utilisées (vulnérabilité sur une fonction serveur alors que vous utilisez uniquement le mode client)

C'est précisément l'analyse de risques qui permet de déterminer l'exploitabilité réelle et de prioriser les actions de remédiation. Les documents VEX (Vulnerability Exploitability eXchange) permettent de communiquer clairement sur le statut de chaque vulnérabilité.

Que faire si je ne peux pas patcher un système legacy ?

Les environnements OT comportent souvent des systèmes legacy qui ne peuvent être mis à jour sans risque de dysfonctionnement. Le CRA reconnaît cette réalité et permet l'utilisation de **mesures compensatoires** :

- **Patching virtuel** : utilisation d'IPS/IDS capable de bloquer les tentatives d'exploitation de vulnérabilités connues, sans modifier le système vulnérable
- **Segmentation réseau** : isolation du système legacy dans une zone sécurisée avec contrôle strict des flux
- **Contrôle d'accès renforcé** : limitation des accès physiques et logiques au système
- **Monitoring intensif** : surveillance accrue pour détecter toute tentative d'exploitation

Ces approches de défense en profondeur permettent de réduire l'exploitabilité des vulnérabilités sans patcher le système lui-même.

Comment gérer le support de sécurité sur 5 ans ?

L'obligation de support minimum de 5 ans représente un changement significatif. Plusieurs stratégies sont possibles :

- **Anticiper dès la conception** : choisir des composants avec un support long terme, concevoir une architecture modulaire facilitant les mises à jour
- **Intégrer le coût dans le modèle économique** : facturer explicitement le support de sécurité, proposer des contrats de maintenance incluant les correctifs
- **Externaliser le PSIRT** : faire appel à un prestataire spécialisé pour la gestion opérationnelle des vulnérabilités et le développement des correctifs
- **Mutualiser les ressources** : pour les PME, des solutions sectorielles de mutualisation commencent à émerger

Le CRA s'applique-t-il aux produits déjà commercialisés ?

Le règlement prévoit un principe de non-rétroactivité : les produits déjà mis sur le marché avant le 11 décembre 2027 ne sont pas soumis aux exigences de conformité initiale. Cependant :

- L'obligation de signalement des vulnérabilités activement exploitées s'applique dès le 11 septembre 2026, **y compris pour les produits déjà commercialisés**
- Les fabricants conservent une obligation générale de sécurité pour les produits en service
- Il est fortement recommandé de fournir des correctifs de sécurité même pour les produits antérieurs, pour des raisons de responsabilité civile et d'image

Puis-je m'appuyer sur des normes pour démontrer ma conformité ?

Oui, le CRA prévoit explicitement l'utilisation de **normes harmonisées**. Lorsqu'une norme harmonisée est publiée au Journal officiel de l'Union européenne, son respect crée une présomption de conformité aux exigences essentielles correspondantes.

Les normes de la série **IEC 62443** (cybersécurité des systèmes d'automatisation et de contrôle industriels) sont particulièrement pertinentes et devraient être harmonisées dans le cadre du CRA :

- IEC 62443-4-1 : exigences pour le développement de produits sécurisés
- IEC 62443-4-2 : exigences techniques de sécurité des composants

D'autres référentiels comme **ISO/IEC 27001** (système de management de la sécurité de l'information) peuvent également contribuer à démontrer la conformité organisationnelle.

Quelles sont les premières actions à entreprendre dès maintenant ?

Pour démarrer efficacement votre démarche :

1. **Inventorier vos produits concernés** et déterminer leur classification CRA
2. **Mettre en place votre point de contact sécurité** (security.txt) pour être joignable dès septembre 2026

3. **Initier l'analyse de risques** sur vos produits prioritaires pour identifier les vulnérabilités et menaces
4. **Former vos équipes** aux enjeux du CRA et aux pratiques de développement sécurisé
5. **Évaluer vos fournisseurs** et intégrer des clauses de sécurité dans vos contrats

Nous vous recommandons de vous faire accompagner pour structurer cette démarche et éviter les erreurs coûteuses.

Conclusion

Le Cyber Resilience Act représente un tournant majeur dans l'approche de la cybersécurité des produits industriels et connectés. Au-delà de la contrainte réglementaire, il constitue une opportunité de différenciation commerciale pour les fabricants qui sauront transformer cette exigence en avantage compétitif.

La conformité CRA nécessite une transformation profonde des pratiques de conception, développement et support des produits. Cette transformation s'inscrit dans la durée et nécessite des investissements significatifs en compétences, processus et technologies. Cependant, elle est incontournable pour continuer à commercialiser sur le marché européen, qui représente un débouché essentiel pour l'industrie manufacturière mondiale.

Les échéances approchent rapidement : septembre 2026 pour le signalement des vulnérabilités, décembre 2027 pour l'ensemble des exigences. Les fabricants doivent agir dès maintenant pour se préparer efficacement. Une approche structurée, basée sur l'analyse de risques et les référentiels reconnus comme IEC 62443, permet de progresser de manière méthodique et d'optimiser les investissements.

Chez AKENATECH, nous accompagnons les industriels dans cette transformation en combinant expertise technique en cybersécurité OT, connaissance des environnements de production et maîtrise des enjeux réglementaires. Notre approche de bout en bout – de la stratégie à l'opération en passant par l'implémentation – vous permet de construire une conformité durable tout en préservant la performance de vos activités.

Ne laissez pas le temps vous échapper. La conformité CRA se construit dès aujourd'hui pour être prêt demain.

Contactez-nous pour échanger sur votre situation spécifique et construire ensemble votre feuille de route de conformité au Cyber Resilience Act.