LE CYBER RESILIENCE ACT

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

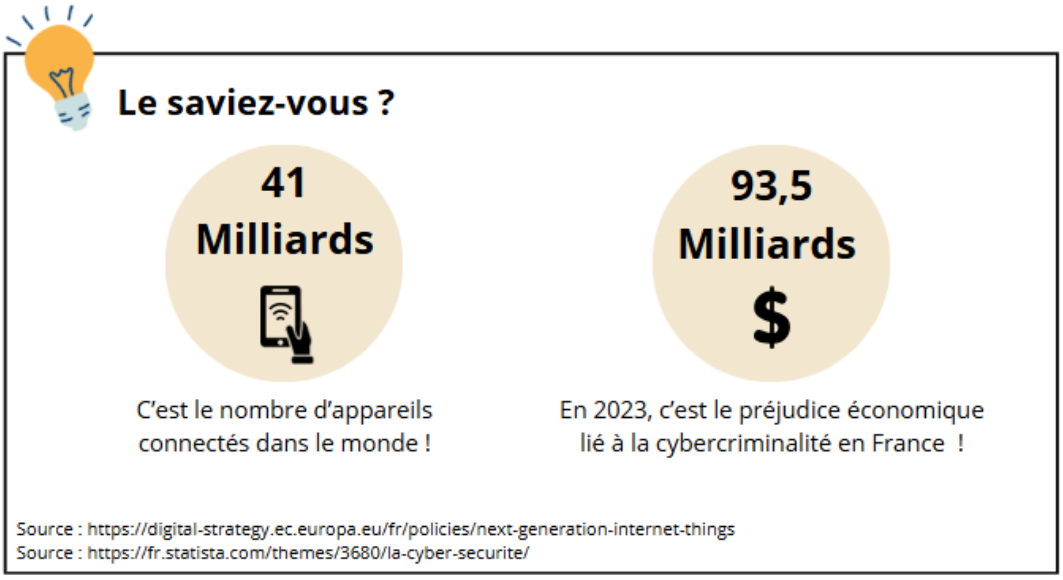
www.csirt-bfc.fr

Sommaire

Qu’est-ce que le Cyber Resilience Act ?

Le Cyber Resilience Act est entré en vigueur **le 10 décembre 2024.** Ce nouveau règlement européen en matière de résilience numérique vient compléter la directive NIS 2 et le règlement DORA.

Il se concentre sur la cybersécurité des produits comportant du numérique mis sur le marché européen ainsi que l’ensemble de la chaine d’approvisionnement.



Quels sont les objectifs du CRA ?

Les objectifs du CRA sont globalement des exigences en matière de cybersécurité sur les appareils. Ex : caméra connectée, réfrigérateur intelligent, brosse à dents connectée, …

Les objectifs principaux :

- Des **règles pour la mise à disposition sur le marché européen** des produits comportant des éléments numériques
- Une **sécurité par défaut** : des exigences en matière de sécurité dès la conception, le développement et la production ainsi que tout au long du cycle de vie du produit
- Des exigences concernant le **processus de gestion des vulnérabilités**
- **Informations** concernant la sécurité du produit avec **une documentation** sur les produits

Les fabricants devront mettre des produits conformes sur le marché de l'UE **d'ici 2027.**

Quelques exceptions…

Certains services ou secteurs sont exclus du périmètre du règlement.

C’est le cas notamment de :

Logiciel fournis en tant que services (SaaS)
Ils sont encadrés par la directive

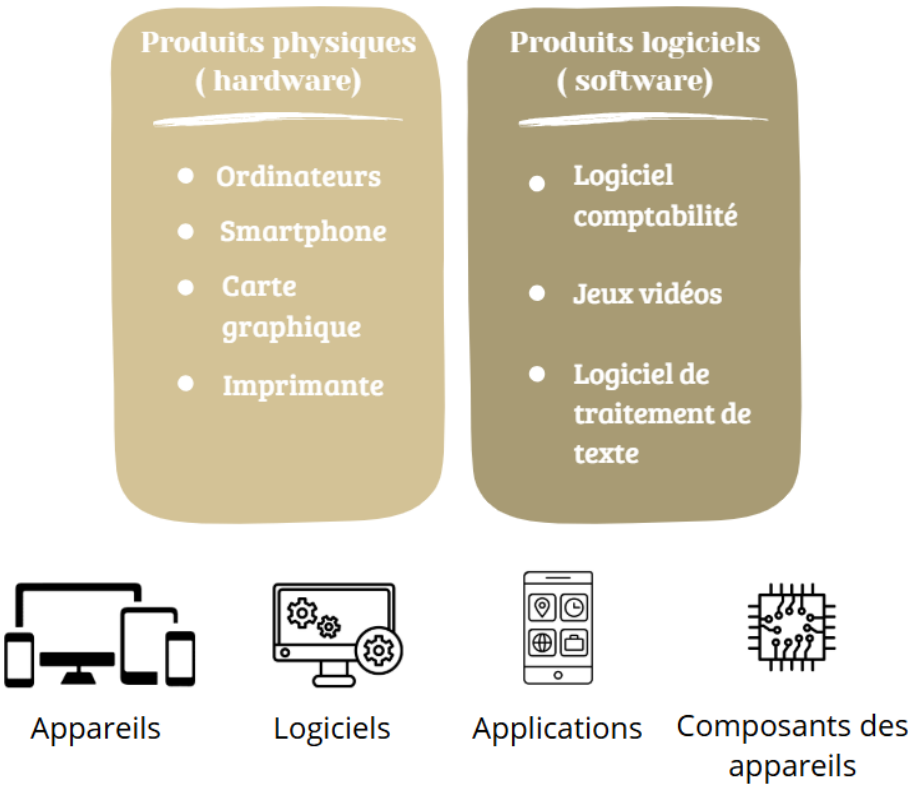
Certains domaines tel que **l’aviation,** les **services médicaux** et les **véhicules à moteurs**

Des produits pour lesquels il existe déjà une **législation européenne spécifique**

Des **produits relevant de la sécurité nationale de l’Etat** ou **traitant des informations classifiées**

Quels sont les produits concernés par le CRA ?

On peut distinguer 2 catégories de produits concernés par le CRA. En voici quelques exemples :



La spécificité de ce règlement c'est que **les logiciels libres ou open-source devront eux aussi respectés le CRA.**

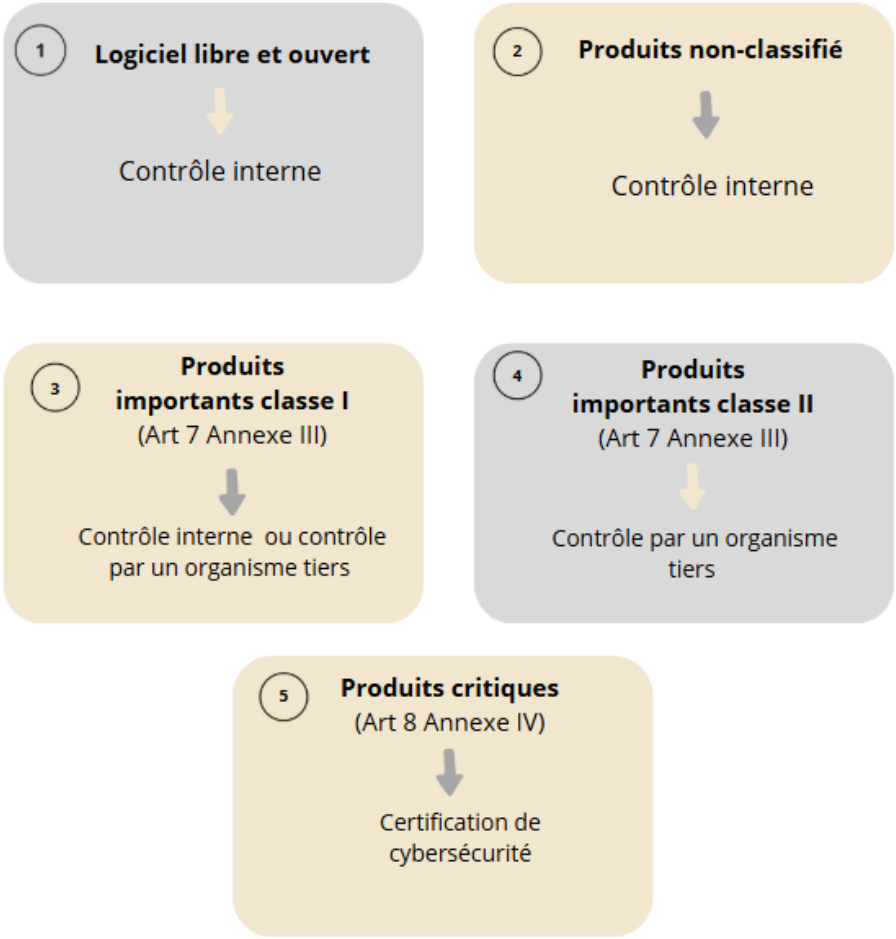
Le règlement définit leurs obligations qui vise à promouvoir une culture de sécurité proactive :

- Politique de cybersécurité définie et claire
- Collaboration avec les autorités pour traiter les risques de sécurité
- Divulgation responsable des vulnérabilités

Le CRA réglemente les produits et non pas les entités !

Chaque produit correspond à une classe qui en fonction de sa criticité adopte une démarche de conformité proportionnelle.

La classe des produits :



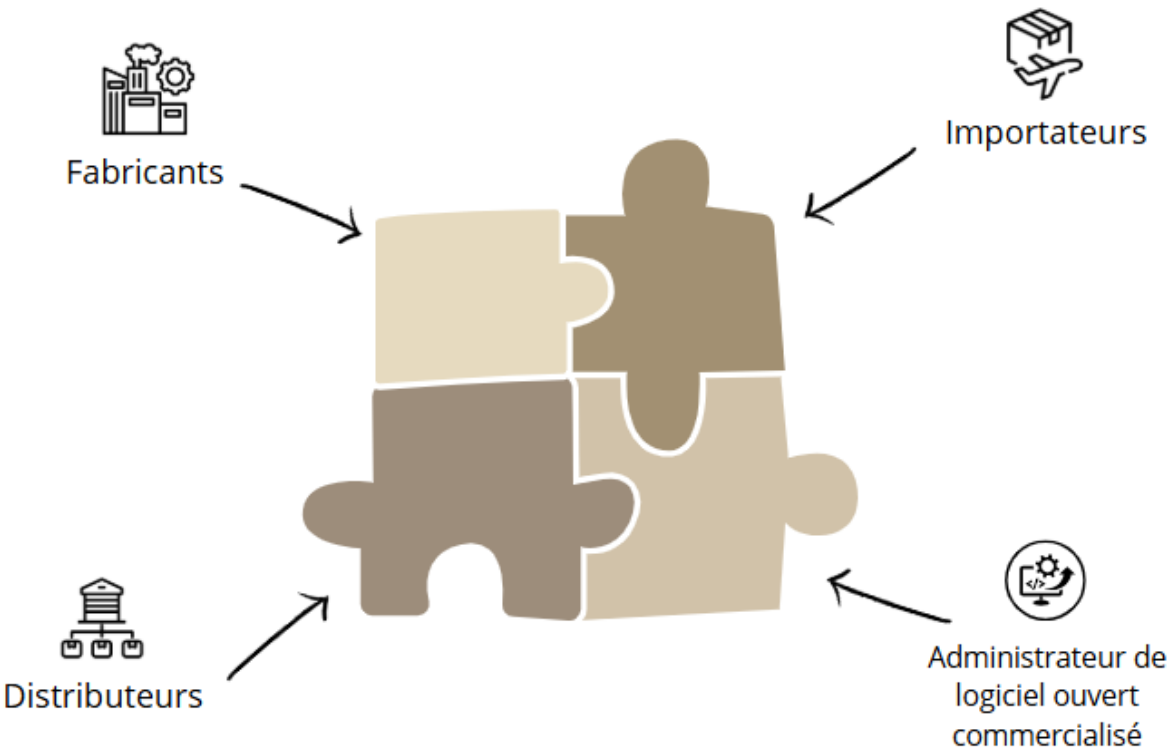
Les systèmes d'IA sont aussi concernés par le CRA **(article 15 du CRA**), il existe une logique de conformité réciproque entre le CRA et l'IA Act. Les systèmes d'IA considérés comme à risque devront être conforme à la fois par l'IA Act mais également par le CRA.

Quels sont les acteurs concernés ?

Les opérateurs économiques qui sont impliqués dans la mise sur le marché et le cycle de vie des produits comportant des éléments numériques.

4 <u>Acteurs :</u>

- Le fabricant du produit numérique ou développeur du logiciel
- L'importateur sur le marché de l'Union européenne lorsque le fabricant est situé hors de l'UE
- Le distributeur et le revendeur
- Administrateur de logiciel ouvert destiné à des activités commerciales

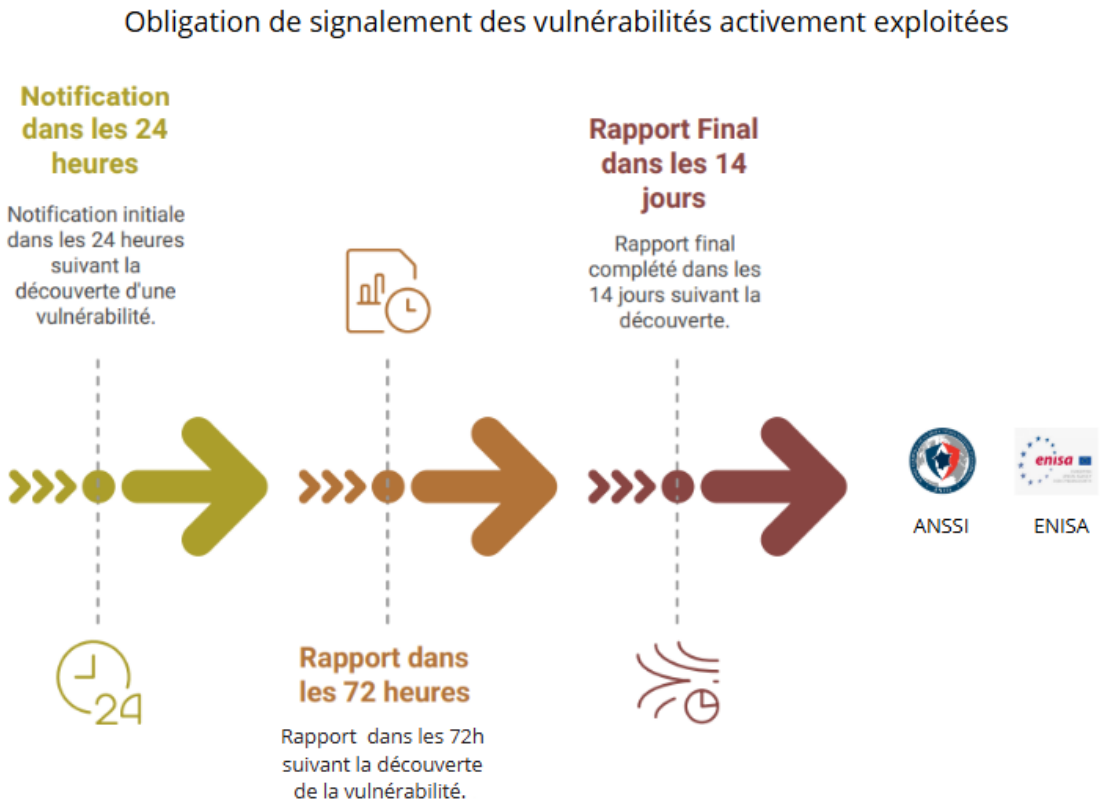


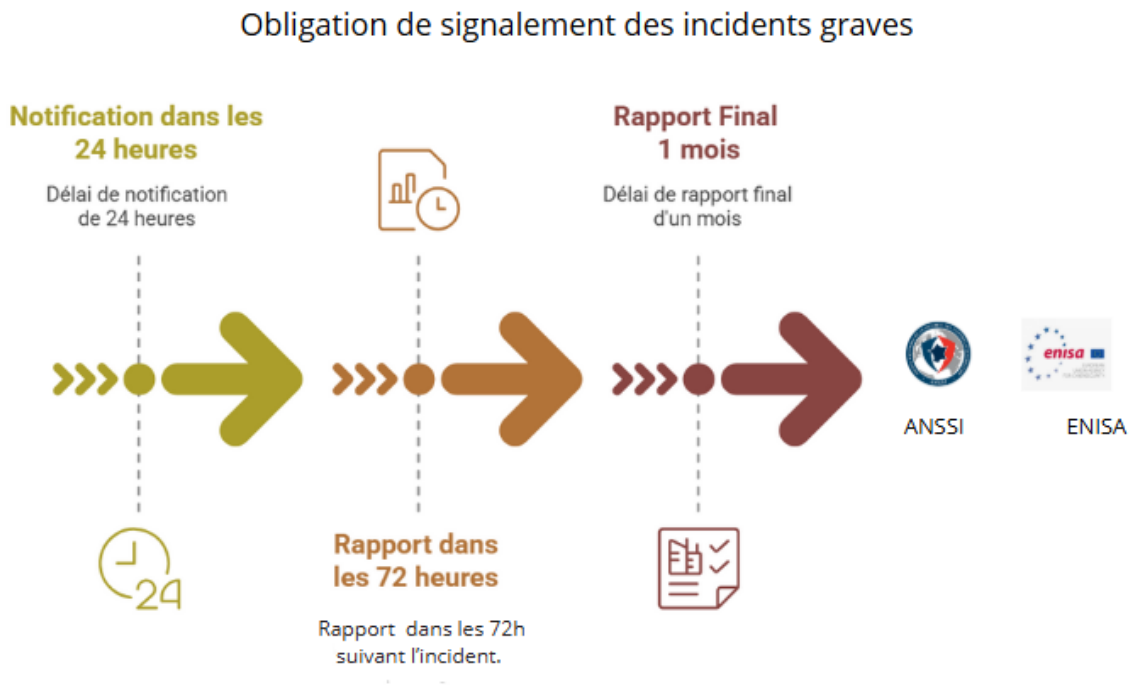
Quelles sont les mesures concrètes à mettre en œuvre ?

Plusieurs mesures sont à mettre en place dans le cadre du CRA :

- L'intégration de la sécurité dès la conception des produits et services (Security by Design)
- La fourniture d'instructions de sécurité claire aux utilisateurs des produits et services
- La mise en place de procédures pour signaler et gérer les incidents de se sécurités liées aux produits et services
- L'obligation de signaler les vulnérabilités qui ont été découvertes dans les 24 heures
- La surveillance post-commercialisation : système de surveillance continue après la mise sur le marché

Il est impératif de notifier les vulnérabilités activement exploitées et les incidents graves à l'ENISA et au CSIRT nationaux donc l'ANSSI dans le cas de la France.





Après avoir rendu le rapport final, le fabricant doit informer les utilisateurs du produit touché.

Durée des correctifs et mises à jour :

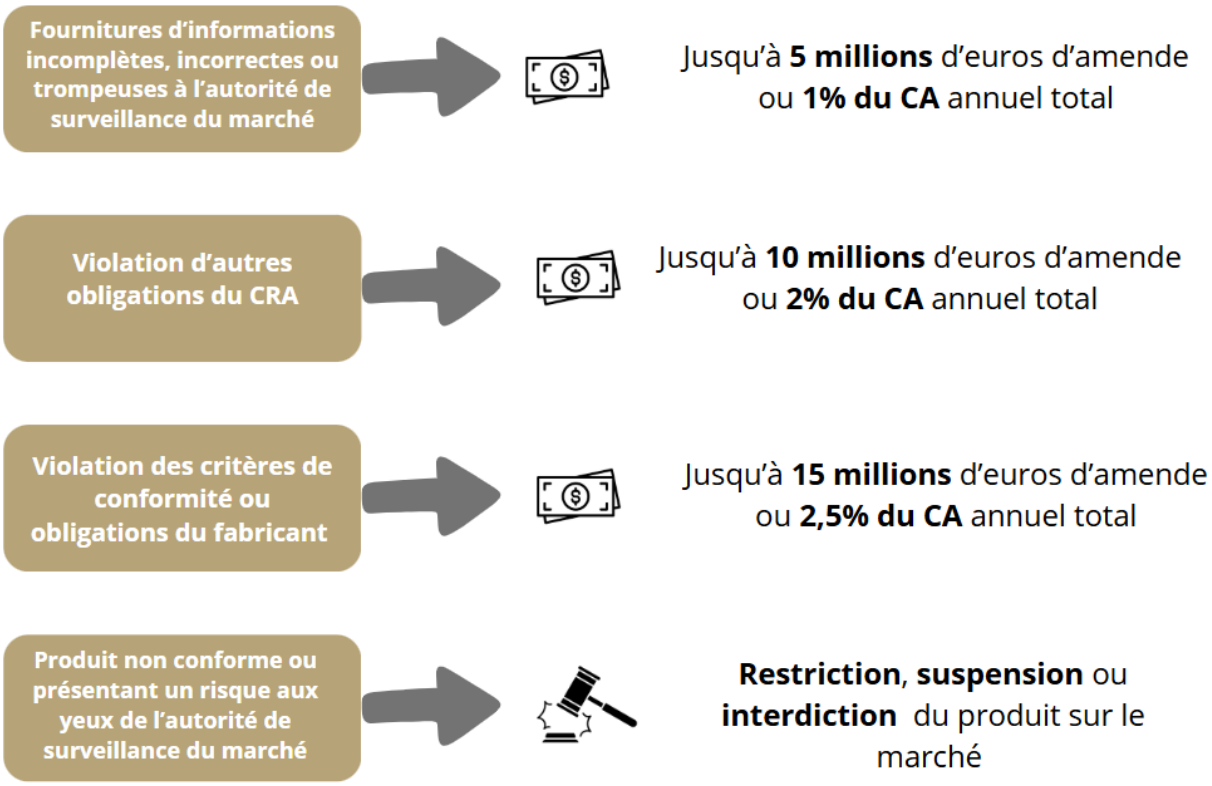
La durée pendant laquelle on doit fournir des correctifs est **de 5 ans.**

Pour les mises à jour de sécurité, il s'agit **de 10 ans**.

Quelles sont les conséquences en cas de violation ?

L'article 64 du CRA prévoit un certain nombre d'amendes administratives.

En cas de violation des critères de conformité, la sanction peut aller jusqu'à **15 millions d'euros** d'amende ou **2,5% du CA** annuel total.



Attention :

Les administrateurs de logiciels open-source ne peuvent pas faire l'objet de sanctions financières.

Les fabricants considérés comme des TPE et micro-entreprises ne seront pas sanctionnés en cas de manquement aux délais de signalement concernant les vulnérabilités et les incidents graves.

Pour plus d'informations voici le lien vers le texte de la Commission Européenne : https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0024.02/DOC_1&format=PDF