CAP'TRONIC
Systèmes électroniques et logiciel embarqué

Impacts de la réglementation cyber dans les produits embarqués et machines industrielles

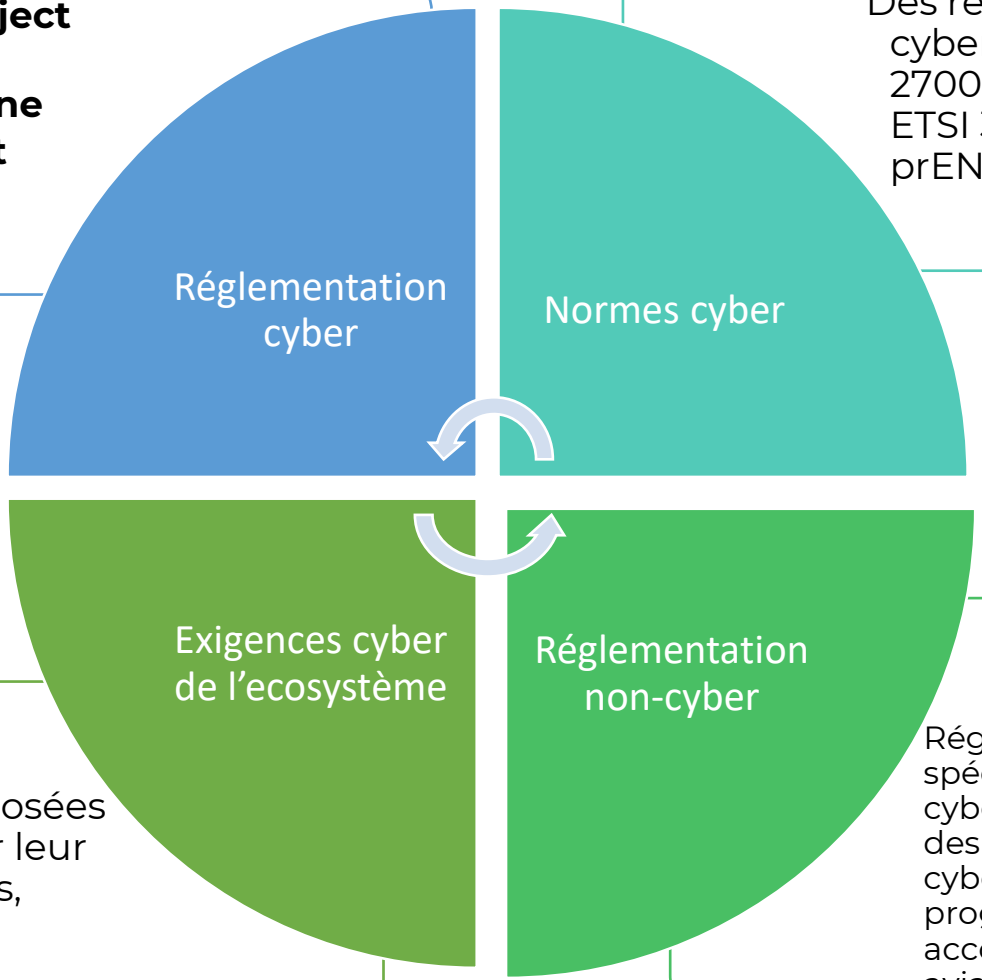
Fondé par : bpifrance cea

05/03/2026

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE
La certification Qualiopi a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION

CONTEXTE REGLEMENTAIRE EN MATIERE DE CYBERSECURITE DES EQUIPEMENTS INDUSTRIELS

- **Directive RED (Object connectés radio)**
- **Règlement machine**
- **Cyber Résilent Act**
- **NIS 2**



Des règles en matière de cybersécurité (ISO 2700x, NIST, IEC 62443, ETSI 303645, EN 18031, prEN50742…)

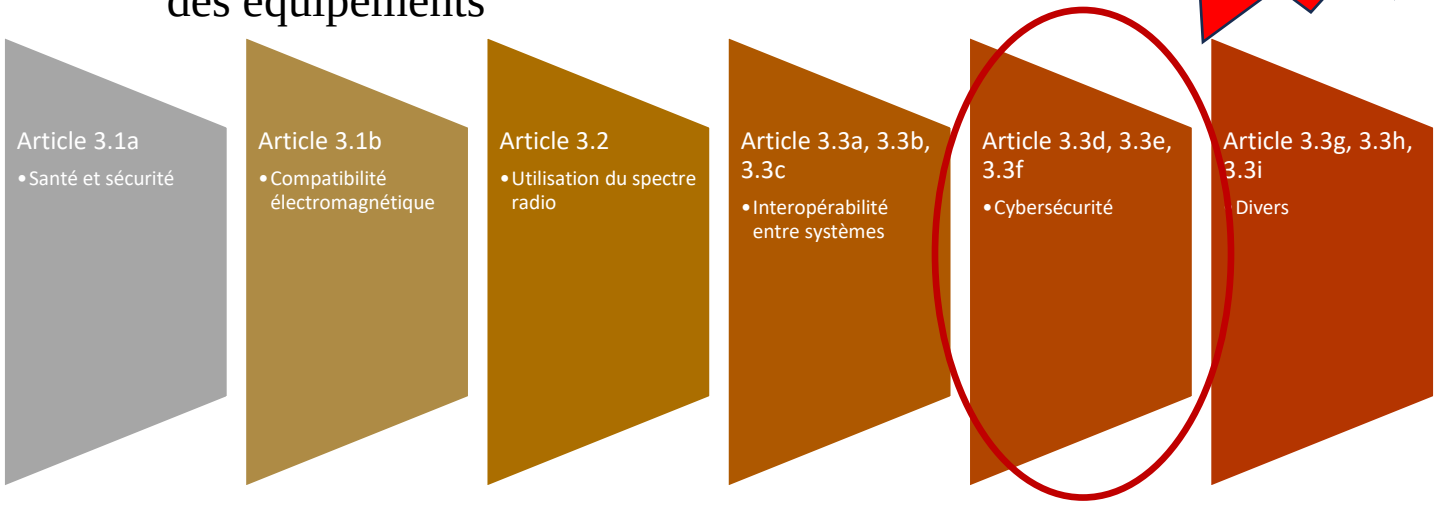
Des contraintes imposées aux entreprises par leur écosystème (clients, partenaires,…)

Réglementations non spécifiques à la cybersécurité mais ayant des impacts sur la cybersécurité. (Loi de programmation militaire, accords de Bâle, normes aviation, DM, ferroviaire,…

Directive Red (Radio Equipement Directive 2014/53/UE) EN 18031

- ✓ Uniformise les exigences pour les équipements radioélectriques
- ✓ Assure la protection de la santé , de la sécurité et de l'environnement
- ✓ Simplifie la circulation des équipements au sein de l'UE
- ✓ Encourage la compatibilité et la coexistence des équipements

Mise en application à partir du 1er Aout 2025



Exigences techniques majeures

Authentification forte

Mécanismes robustes d'authentification et contrôle d'accès

Mises à jour sécurisées

Processus garantissant l'intégrité et l'authenticité des mises jour logicielles

Protection des données

Stockage et communication sécurisés des informations sens

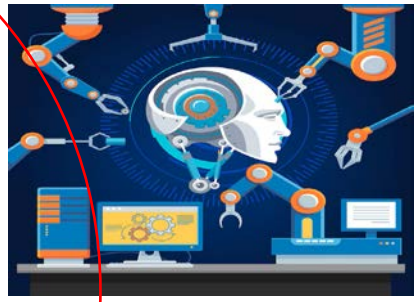
Résilience DoS

Résistance face aux attaques par déni de service

LE NOUVEAU REGLEMENT MACHINE : Changements fondamentaux

Mise en application à partir du 20 janvier 2027

Intégration d'exigences relative à la cybersécurité



Prise en compte de l'usage de l'IA

Numérisation de la documentation

Nouvelles exigences essentielles de santé et sécurité

Nouveaux risques intégrés

- Intelligence artificielle
- Cybersécurité industrielle
- Internet des objets (IoT)
- Connectivité des machines

Risques traditionnels maintenus

- Vibrations et bruit
- Substances dangereuses
- Sécurité mécanique
- Ergonomie et interfaces

Les exigences de conception et construction sont renforcées pour tenir compte de l'évolution technologique tout en conservant la protection contre les risques classiques.

Responsabilités renforcées

Fabricants

Obligations étendues de conception, évaluation de conformité et traçabilité complète des machines produites.

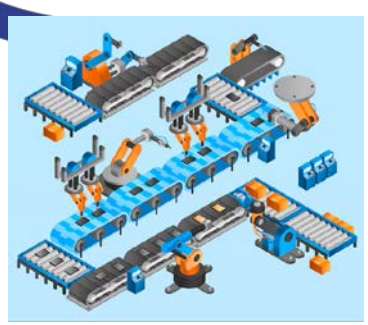
Importateurs

Vérification de la conformité, étiquetage correct et responsabilité sur le marché européen.

Distributeurs

Contrôle du respect des exigences et coopération avec les autorités de surveillance.

Le nouveau règlement sur la sécurité des machines : Intégration de dispositions relative à la cybersécurité



Ne pas créer de situations dangereuses lorsque les machines sont connectées entre elles

Assurer, en toutes sécurité, l'intégrité, la confidentialité et la disponibilité des données en transit au sein des processus industriels
Protéger les données de manière adéquate contre la corruption accidentelle ou intentionnelle

Identification des logiciels installés
Permettre au client d'accéder aux différents niveaux des mises à jour des logiciels installés
Disposer d'un historique des évènements (recueille de preuve légitime ou illégitime d'interventions, mises à jour, changement de paramètres,…)

Des mots clés importants dans PROJET DE NORME EN 50742

CORRUPTION:
action accidentelle et intentionnelle (y compris malveillante) sur des machines pouvant entrainer des situations dangereuses

PREUVE:
Tout ce qui permet de détecter qu'un événement ou une action s'est produite

INTERVENTION :
Action/évènement légitime ou illégitime qui modifie le logiciel ou les données et modifie ou interrompt temporairement ou définitivement le comportement ou l'état de fonctionnement de la machine

LES INTERVENTIONS selon PROJET DE NORME EN 50742

- ✓Paramétrage de sécurité
- ✓Mise à jour/modification du logiciel embarqué de sécurité
- ✓Mise à jour/modification du logiciel applicatif de commande de sécurité
- ✓Paramétrage des IHM si cela peut provoquer un risque (risque opérateur)
- ✓Logiciel pour l'affichage des consignes de sécurité

LES PREUVES selon le projet de norme EN 50742

Action qui modifie ou interrompt le fonctionnement de la machine ou qui modifie le logiciel et les données :

- Le type d'intervention qui affecte le logiciel utilisé pour la réduction des risques
- Les moyens permettant de corréler les évènements
- Les tentatives de suppression du fichier journal

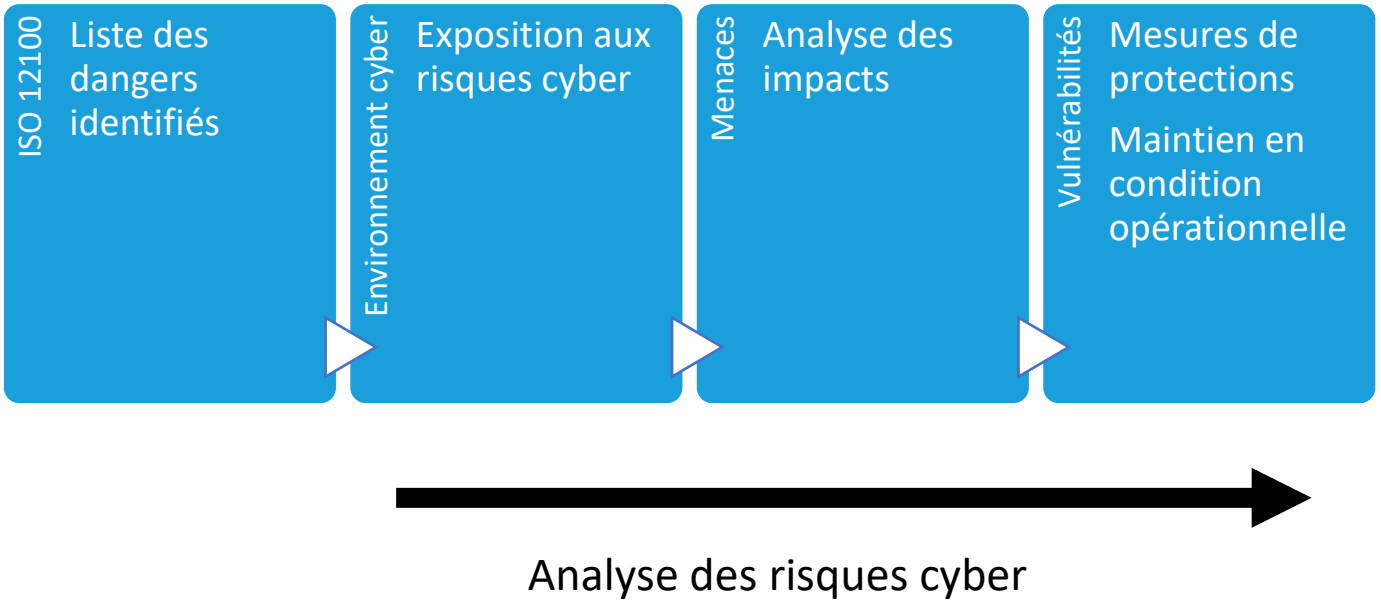
Durée

- Journalisation activée à la mise en service
- Au minimum les preuves des dernières interventions
- Conservation du journal pendant au moins 5 ans

Protection

- Le journal doit être sécurisé afin d'empêcher toute falsification
- La suppression des journaux ne doit être possible que par une procédure autorisée et documentée

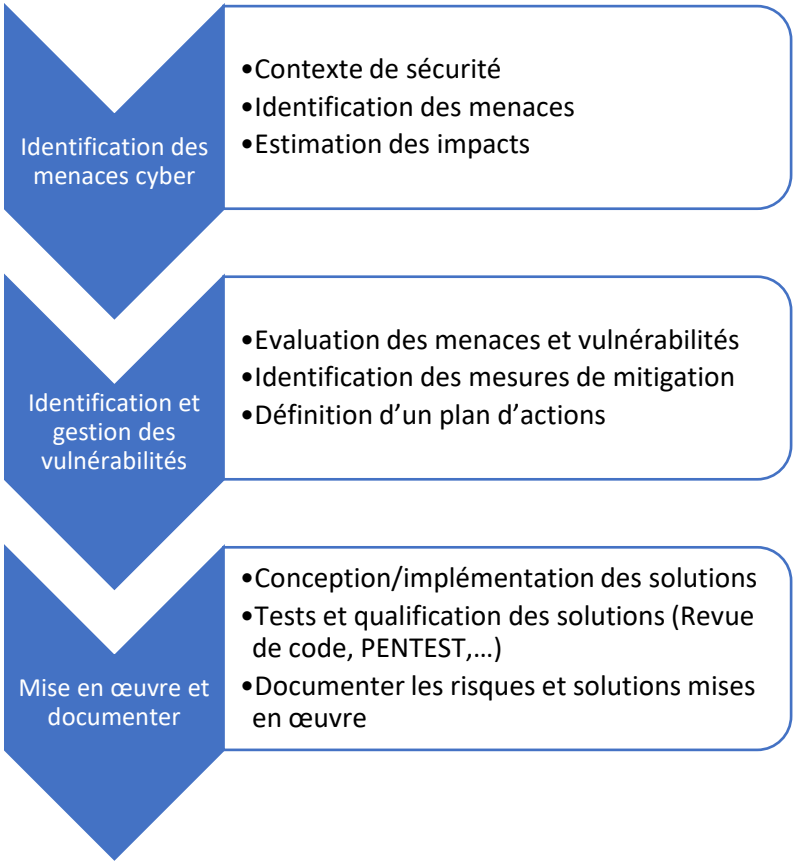
ELARGISSEMENT DE L'ANALYSE DES RISQUES



APPROCHE « A » de l'EN 50742

Approche A

vise à prévenir toute corruption des machines entrainant des situations dangereuses



DES EXIGENCES ADAPTEES pour l'approche A

Système complètement isolé — Confiance forte : faible probabilité d'attaque — Confiance modérée : forte probabilité d'attaque — ***Réseau non fiable***

	SRSL0	SRSL1	SRSL2	SRSL3
Identification/Authentification		Accès par un mécanisme d'identification global	Accès par un mécanisme d'identification global	Accès par des mécanismes d'authentifications individuelles
Autorisation		Vérification globale des droits d'accès (opération admise)	Vérification globale des droits d'accès (opération admise)	Vérification des accès selon les droits attribués
Intégrité logicielle		Mécanisme de vérification au démarrage	Vérification de l'intégrité logicielle de manière périodique	Vérification permanente de l'intégrité logicielle
Intégrité du processus de démarrage		Mécanisme de vérification au démarrage	Mécanisme de vérification au démarrage	Vérification de l'intégrité du processus d'amorçage au démarrage
Intégrité dans les échanges d'informations		Mise en place des mécanismes vérifiant l'intégrité des informations	Mise en place des mécanismes vérifiant l'intégrité des informations	Mise en place des mécanismes de chiffrement
Saisie des données		Validation simple selon le contexte d'utilisation	Validation de la syntaxe, la longueur et le contenu des données d'entrée utilisées	Validation contextuelle des données saisies
Altération physique		Détection simple d'un évènement	Détection simple d'un évènement	Détection simple d'un évènement
Authenticité des logiciels			Utilisation des mécanismes basés sur des clés/signatures	Utilisation des mécanismes basés sur des clés/signatures
Versions et configuration des logiciels		Sur demande		

APPROCHE « B » de l'EN 50742

Approche B

Suivi des exigences issues de l'IEC 62443 :

IEC 62443 4.1: Secure by design

IEC 62443 3.3 : Sécurité des réseaux

IEC 62443 4.2 : Exigences produits

IEC 62443 4.1

IEC 62443 3.3

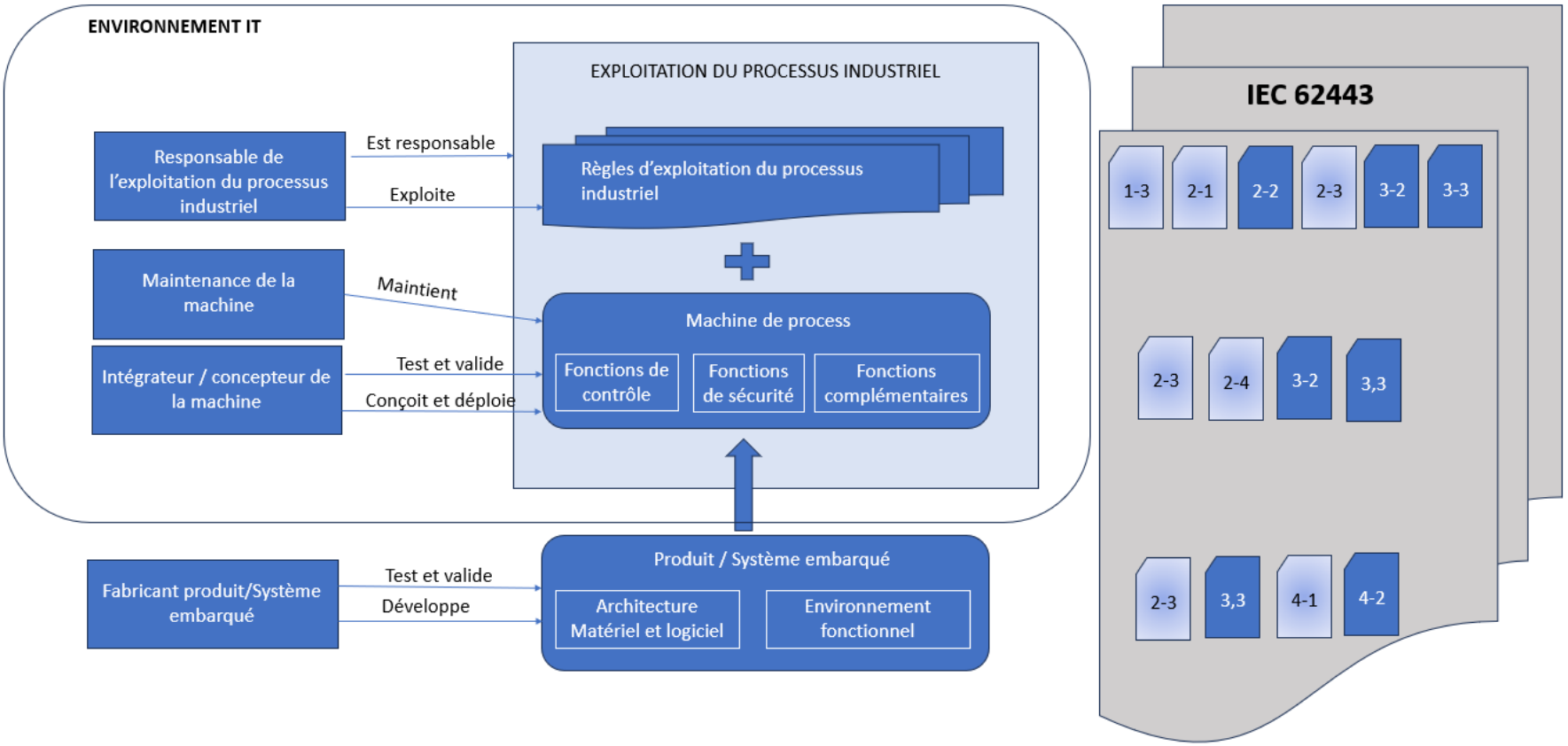
- FR 1 – Identification et contrôle de l'authentification
- FR 2 – Contrôle de l'utilisation
- FR 3 – Intégrité du système
- FR 4 – Confidentialité des données
- FR 5 – Flux de données restreint
- FR 6 – Réponse rapide aux événements
- FR 7 – Disponibilité des ressources

IEC 62443 4.2

- FR 1 – Identification et contrôle de l'authentification
- FR 2 – Contrôle de l'utilisation
- FR 3 – Intégrité du système
- FR 4 – Confidentialité des données
- FR 5 – Flux de données restreint
- FR 6 – Réponse rapide aux événements
- FR 7 – Disponibilité des ressources

REGLEMENT MACHINE ET CONVERGENCE IT/OT

Convergence IT /OT dans le cadre de l'IEC62443



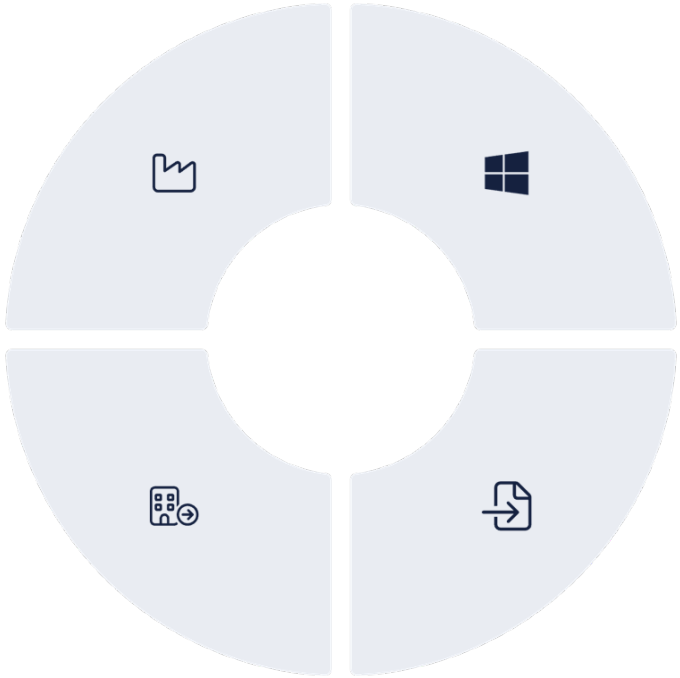
CONSEQUENCES POUR LES INDUSTRIELS

Fabricants

Responsabilité complète de la conformité réglementaire et de l'intégration native de la sécurité

Distributeurs

Contrôle et validation de la conformité des machines distribuées



Opérateurs

Responsables de la **maintenance continue** et sécurité opérationnelle

Importateurs

Vérification obligatoire de la conformité avant **mise sur le marché européen**

Normes et bonnes pratiques

Une approche par les processus permettant de se préparer au Cyber Résilient Act

Cartographie de l'équipement :
- **Nomenclature produits**
- **Nomenclature logicielles**
- **Architecture réseaux**

Processus de secure by design

Documentations :
- **Technique**
- **Processus**
- **Gestion des mises à jour**

Appréciation du risque selon l'EN ISO 12100

Processus d'analyse des risques

Mise en place d'un processus de gestion des vulnérabilités

Choix entre approche A ou B + analyse des risques de cybersécurité

Socle de sécurité

Tests et validation :
- **PENTEST**
- **Qualification logicielle**

Normes et bonnes pratiques

Normes IEC 62443

Recommandées officiellement pour la cybersécurité industrielle et l'intégration dans les machines connectées

Protocoles sécurisés

OPC UA avec TLS, Profisafe, CIP Safety pour des **communications fiables et chiffrées**

Approches intégrées

"Defense in Depth" et "Secure by Design" pour garantir une robustesse maximale

Cyber Resilience Act, un règlement horizontal !

Pour les fabricants de produits numériques (IoT, logiciels…) connectés

- ✓ Règlement européen,
- ✓ Imposer des mesures **à respecter par les constructeurs** dès la conception des produits
- ✓ Tout type de **hardware** (routeurs, switchs, disques durs, caméras, smartphones, enceintes connectées, IoT, etc.) et de **software** (logiciel de traitement de texte, antivirus, logiciels VPN, OS serveurs) + logiciel Open Source (si commercialisé)

Les fabricants devront notamment développer, documenter et mettre en œuvre des politiques et des procédures pour chaque projet, préparer une documentation technique pour chaque version de produit et suivre un processus de marquage CE.

- ✓ **Prendre en compte la cybersécurité dans toutes les phases** de *conception*, de *développement*, de *production*, de *livraison* et de *maintenance* de leurs produits ;
- ✓ **Sourcer les composants électroniques qu'ils intègrent** afin de se s'assurer qu'ils ne compromettent pas la sécurité de leurs produits ;
- ✓ **Évaluer et documenter tous les risques cyber** pertinents et identifiés liés à ses produits
- ✓ **Fournir aux acheteurs une documentation évaluant les risques cyber** de leurs produits
- ✓ **Corriger les vulnérabilités cyber de leurs produits pendant leur durée de vie ou pendant 5 ans** à compter de leur mise sur le marché;
- ✓ **Signaler les vulnérabilités** et les incidents

Mise en application à partir du 11 décembre 2027

DATES IMPORTANTES

Le CRA ..une mise en œuvre progressive…

11 juin 2026 : application aux organismes en charge de l'évaluation des conformités.
les pays de l'UE doivent désigner les "organismes autorisés à procéder à l'évaluation de la conformité CRA.

11 septembre 2026 : entrée en vigueur des obligations de notifications des vulnérabilités des systèmes par les fabricants
les "vulnérabilités activement exploitée des produits et systèmes commercialisés doivent être identifiées et corrigées (si c'est possible)
Les "incidents de sécurit ayant des répercussions sur la sécurité des produits et logiciels connectés devront être notifications aux autorités (ENISA + CERT national) mais aussi il faudra informer les particuliers comme professionnels :

A partir du 11/12/2027

- 24h pour une alerte précoce dès la détection
- 72h pour une notification complète avec évaluation initiale
- 14 jours pour le rapport final sur une vulnérabilité (une fois le correctif disponible)

11 décembre 2027 : entrée en vigueur du CRA dans sa totalité.

TOUS les fabricants et importateurs de PRODUITS connecté ***commercialisés AVANT le 11 décembre 2027 devront,*** *à compter du 11 décembre 2027,* ***avoir mis en place une procédure de notification*** *des vulnérabilités connues et des incidents de sécurité ayant des répercussions sur la sécurité*

CRA – Mode d'emploi

Cartographier chaque « produit comportant des éléments numériques » et le classer (annexe III Classe I/II).

- ✓ Intégrer l'analyse des risques dans le SDLC
- ✓ Automatisez le SBOM et le scanner de vulnérabilité Définir un socle de sécurité réglementaire :ETSI EN 303 645 - EN 18031 - IEC 62443 – EN50742
- ✓ Former les équipes sur le flux de travail de divulgation coordonné
- ✓ Examinez les composants tiers pour obtenir la preuve du marquage CE (prise en compte de la cyber)
- ✓ Prévoyez dès maintenant un budget pour l'évaluation externe de la conformité.

Bonnes pratiques : NIS2 = niveau opérationnel et CRA = au niveau du produit

- ➢ **Traitez-les comme des piliers de votre stratégie de cybersécurité.**

UNE CLASSIFICATION DES PRODUITS

Le Cyber Resilience Act distingue **quatre catégories** parmi les produits embarquant du numérique qu'il réglemente :

- ✓ **La catégorie par défaut,** qui n'est pas mentionnée en tant que telle, mais qui existe de facto. Elle comprend tous les produits qui répondent aux définitions générales: *« Produit comportant des éléments numériques' : tout produit logiciel ou matériel et ses solutions de traitement des données à distance, y compris les composants logiciels ou matériels devant être mis sur le marché séparément."* ***– CRA, Article 3 »***

- ✓ **Les produits importants de Classe I** ;

Produits dont la fonctionnalité coeur est jugée importante pour la cybersécurité

- ✓ **Les produits importants de Classe II**;

Sous-ensemble plus sensible des produits importants, qui déclenche des exigences d'évaluation plus contraignantes.

- ✓ **Les produits critiques**.

Catégories les plus sensibles qui requièrent en principe une évaluation tierce (ou certification) avant mise sur le marché.

Il est essentiel de bien comprendre cette classification, car elle détermine, entre autres, la procédure d'évaluation de la conformité attendue pour chaque produit.

Ainsi, plus le produit est critique, plus l'évaluation sera rigoureuse – comprenez ici l'intervention d'un auditeur tiers.

LES EXIGENCES ESSENTIELLES DU « CRA »

- ✓ **Être mis à disposition sur le marché sans vulnérabilité exploitable connue** ;
- ✓ **Être mis à disposition sur le marché avec une configuration sécurisée par défaut**
- ✓ **Garantir que les vulnérabilités peuvent être corrigées par des mises à jour de sécurité**
- ✓ **Assurer la protection contre les accès non autorisés au moyen de mécanismes de contrôle appropriés**
- ✓ **Protéger la confidentialité des données** stockées, transmises ou traitées
- ✓ **Protéger l'intégrité des données** stockées, transmises ou traitées
- ✓ **Ne traiter que des données, personnelles ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire** au regard de la finalité du produit ("minimisation des données") ;
- ✓ **Protéger la disponibilité des fonctions essentielles et basiques,** y compris après un incident, notamment par des mesures de résilience et d'atténuation des attaques par déni de service (DDoS) ;
- ✓ **Minimiser l'impact négatif des produits eux-mêmes ou des dispositifs connectés** sur la disponibilité des services fournis par d'autres dispositifs ou réseaux ;
- ✓ **Être conçus, développés et produits de manière à limiter les surfaces d'attaque,** y compris les interfaces externes ;
- ✓ **Être conçus, développés et produits de manière à réduire l'impact d'un incident** à l'aide de mécanismes et de techniques d'atténuation de l'exploitation appropriés ;
- ✓ **Fournir des informations relatives à la sécurité en enregistrant et/ou en surveillant l'activité interne** pertinente
- ✓ **Donner la possibilité aux utilisateurs de supprimer de manière sûre, simple et permanente toutes les données et tous les paramètres** et, lorsque ces données peuvent être transférées à d'autres produits ou systèmes, veiller à ce que cela se fasse de manière sécurisée.

Défis pour fabricants et développeurs

Secure by Design

Intégrer la cybersécurité dès les premières phases de conception nécessite une refonte complète des processus de développement traditionnels.

Équilibre coût-risque

Trouver le juste équilibre entre les investissements techniques en sécurité et l'évaluation réaliste de l'impact des risques cyber.

Cycle de vie étendu

Gérer la sécurité sur des décennies d'utilisation, avec des contraintes de maintenance et d'évolution technologique.

Compétences spécialisées

Former les équipes et favoriser la collaboration entre experts sécurité, développement et métier.

CRA : Bonnes pratiques recommandées

Évaluation des risques

Risk assessment systématique et analyse des menaces

Travail sur les données

Confidentialité, Intégrité, Disponibilité

Détection & Réponse

Mécanismes d'incident response

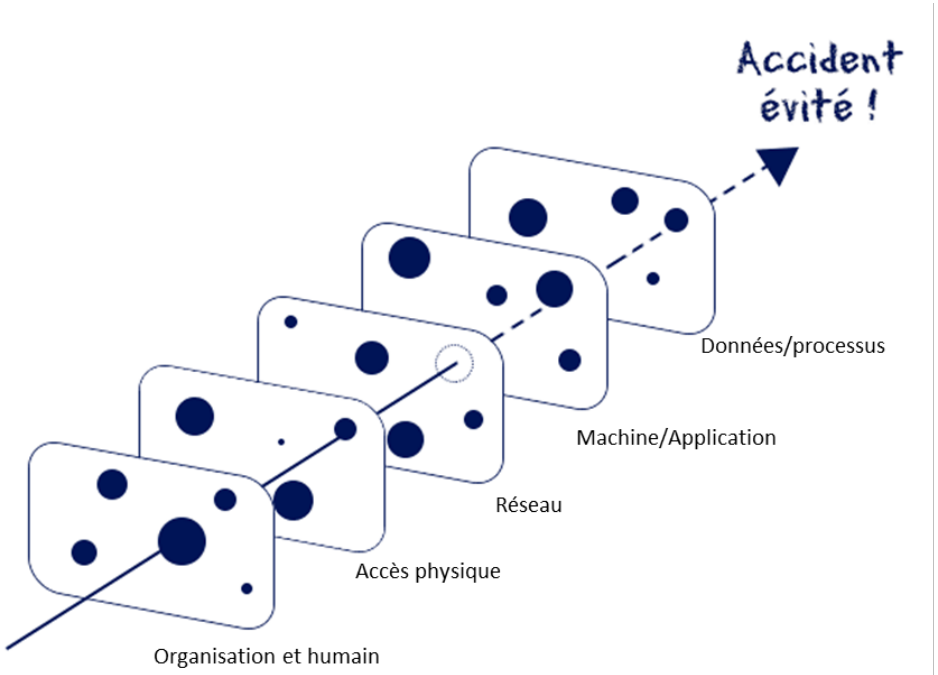
Surface d'attaque

Limitation et configuration sécurisée

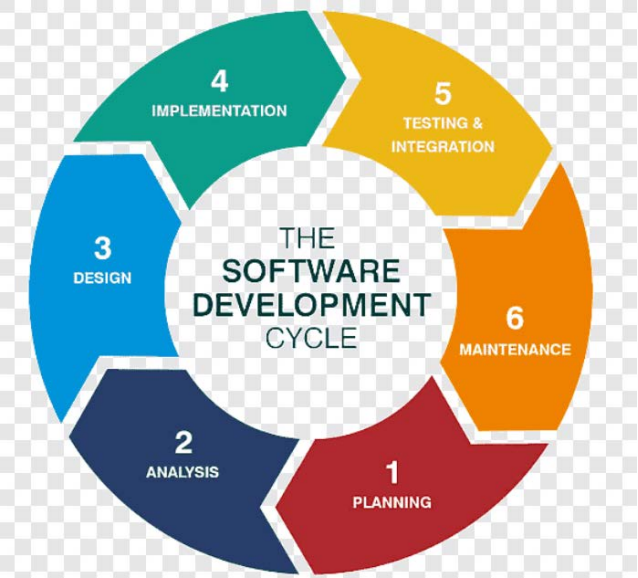
POUR RESUMER …

C'EST donc LA CHAÎNE COMPLÈTE QU'IL FAUT SÉCURISER !

Appliquer la stratégie de Vauban avec plusieurs niveaux de protection



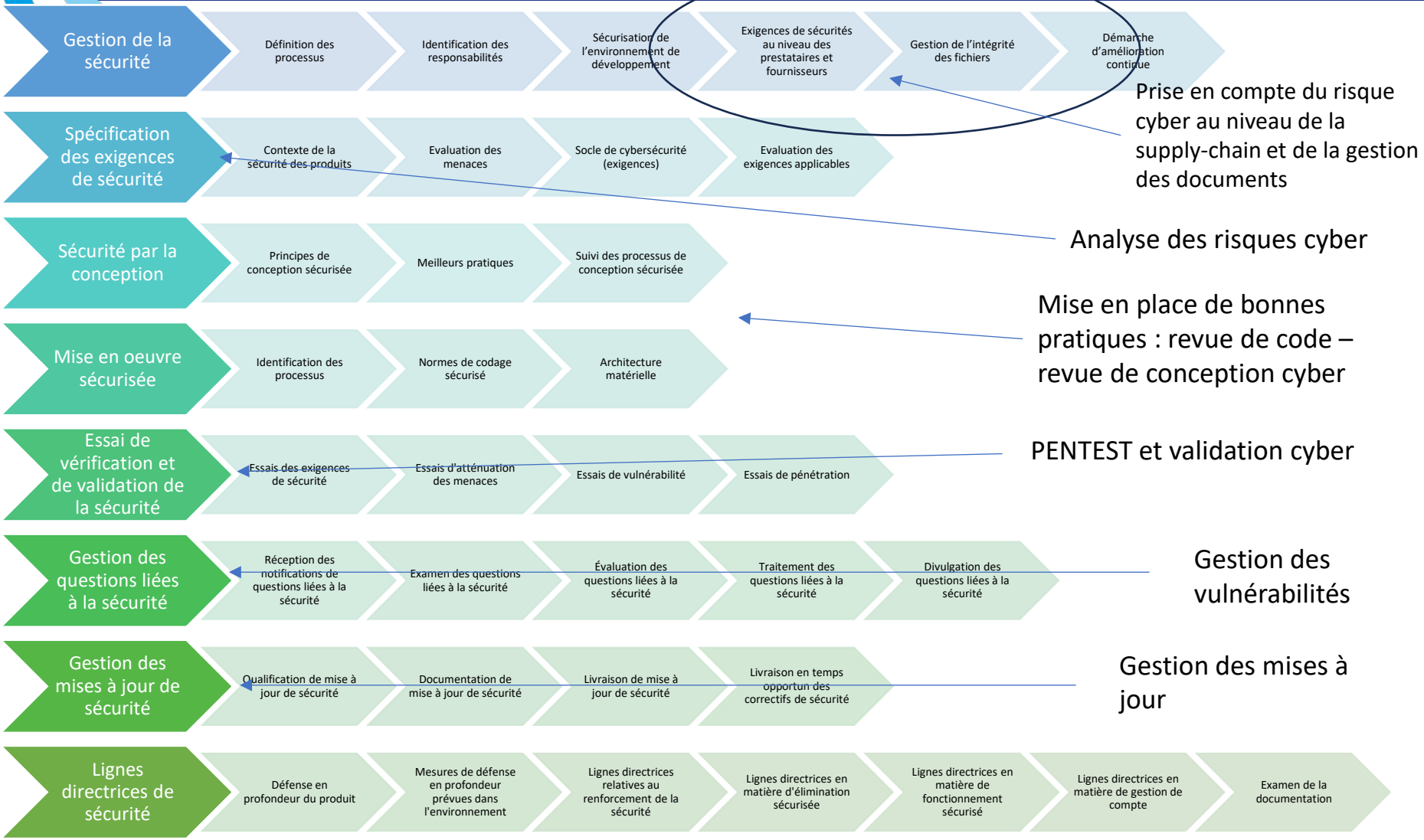
SECURE BY DESIGN ou la cybersecurité dés la conception



La **sécurité dès la conception** est l'intégration de la sécurité dès la conception d'un système (début du cycle de vie).

Elle tient compte des risques et nécessite un travail d'équipe multidisciplinaire et une stratégie de sécurité claire

Maitrise des processus du « secure by design »



Prise en compte du risque cyber au niveau de la supply-chain et de la gestion des documents

Analyse des risques cyber

Mise en place de bonnes pratiques : revue de code – revue de conception cyber

PENTEST et validation cyber

Gestion des vulnérabilités

Gestion des mises à jour

Mettre en place une analyse des risques cyber

- Identifier les vulnérabilités et menaces spécifiques à l'organisation ou au système

- Évaluer l'impact potentiel sur les actifs critiques (données, systèmes, réputation)

- Prioriser les actions pour optimiser les ressources de cybersécurité

La gestion des risques, une affaire de méthodes

Méthodes générales d'analyse des risques

EBIOS RM
- Méthode française de référence
- Analyse par **scénarios de risques**
- Axée sur les **objectifs métiers** et les **sources de menace**

ISO IEC 27005
- Standard international
- Cadre méthodologique pour la gestion du risque SI
- Souple et s'adapte à différents contextes

MEHARI
- Approche qualitative et quantitative
- Outils de notation et tableaux de bord
- Adaptée aux SI complexes

Méthodes orientées menaces et attaques

EBIOS RM

STRIDE
- Axée sur les types d'attaques
- Très utilisée pour l'analyse applicative

PASTA
- Méthode orientée attaque
- Combine business, technique et menaces
- Adapté aux environnements applicatifs

Méthodes quantitatives / semi-quantitatives

FAIR
- Méthode quantitative (en € / impact financier)
- Très utilisée pour le **risk-based decision making**
- Excellente pour convaincre la direction

CRAMM
- Méthode britannique
- Très structurée et détaillée
- Moins utilisée aujourd'hui

Méthodes complémentaires

Analyse de scénarios
- Construction de scénarios d'attaques plausibles
- Très efficace en ateliers métiers / RSSI

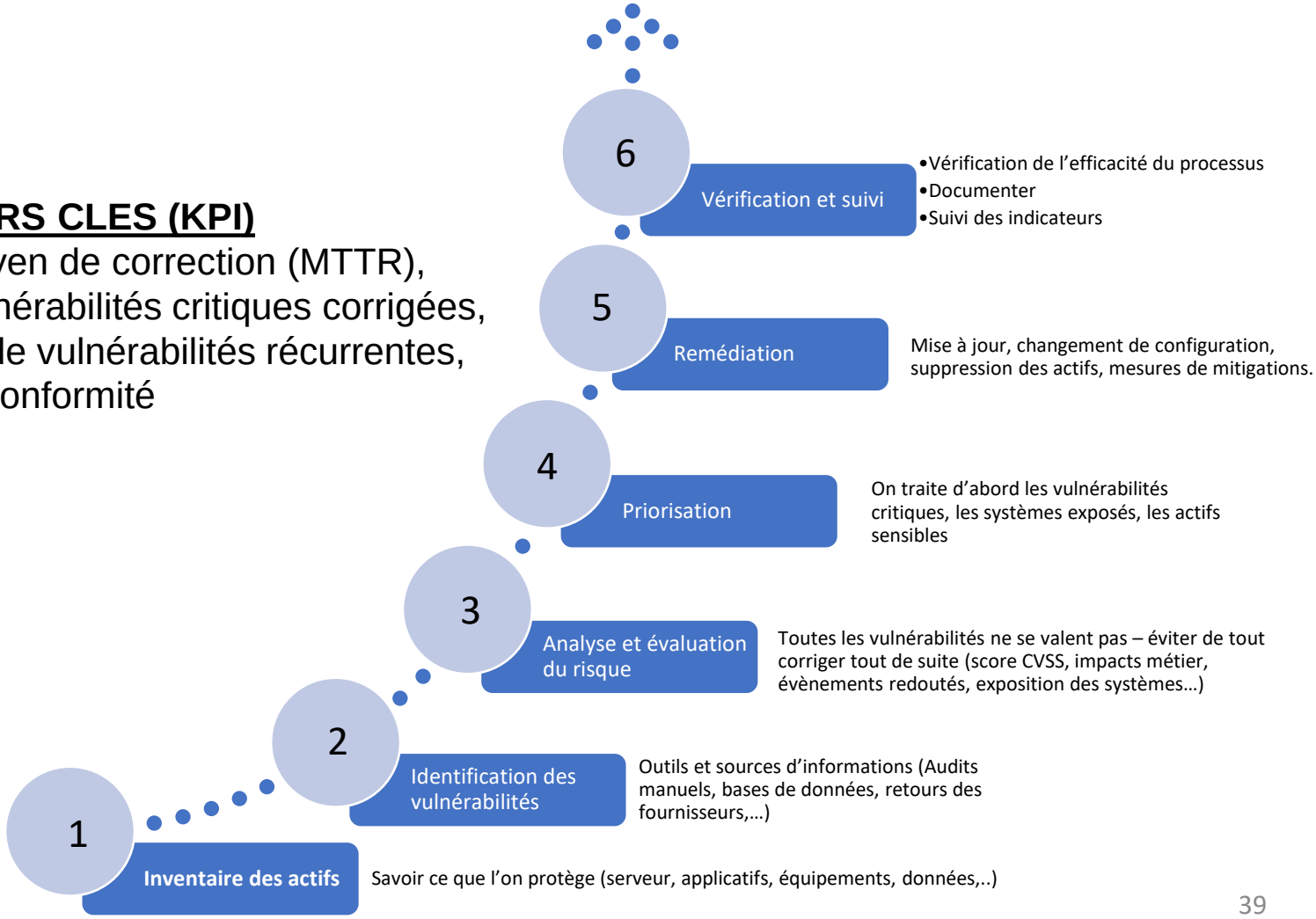
Cartographie des risques
- Visualisation des risques (probabilité × impact)
- Complément indispensable à toute méthode

Threat Modeling
- Approche globale (souvent combinée avec STRIDE, PASTA)
- Très utilisée en DevSecOps

Mettre en place un processus de gestion des vulnérabilités

INDICATEURS CLES (KPI)

- ✓ délai moyen de correction (MTTR),
- ✓ % de vulnérabilités critiques corrigées,
- ✓ nombre de vulnérabilités récurrentes,
- ✓ taux de conformité



Bonnes pratiques

- ✓ processus continu (pas un scan annuel)
- ✓ collaboration IT / Sec / Dev
- ✓ automatisation quand possible
- ✓ intégration DevSecOps
- ✓ documentation et traçabilité
- ✓ Mise en place d'une SBOM

C'est un fichier qui contient la liste des dépendances de l'application, qu'elles soient directes ou indirectes. Mettre en place une SBOM, c'est identifier la liste de toutes les bibliothèques embarquées par une application.

Mettre en place un processus de revue de code

La revue de code se positionne comme une étape incontournable dans le processus de développement logiciel, et ce, quelle que soit la taille du projet

Les revues de code permettent de garantir la qualité du logiciel, partager les connaissances au sein de l'équipe et favoriser la collaboration. Elles contribuent à la détection précoce des erreurs, à l'amélioration des compétences des développeurs et à la cohérence du code au sein d'un projet.

1 000 lignes de codes génèrent en moyenne 0,03 à 0,05 vulnérabilité soit, pour un équipement de 1 à 5 M de lignes de codes, 30 à 150 vulnérabilités

- ✓ Attention aux débordements
- ✓ Attention aux pointeurs libérés (et pointeurs invalides)
- ✓ Attention aux changements du chemin normal d'exécution (détournement de flot et injection de code)
- ✓ Attention à l'utilisation de données non initialisées (variable non assignée à une valeur)

Bonnes pratiques

- Le standard Misra C est **une référence dès que la sécurité du code est importante.**

MISRA comprend un ensemble de paramètres et de règles de codage ainsi que des supports (informations de base permettant la certification du code)
Deux solutions sont possibles pour intégrer MISRA à un développement :

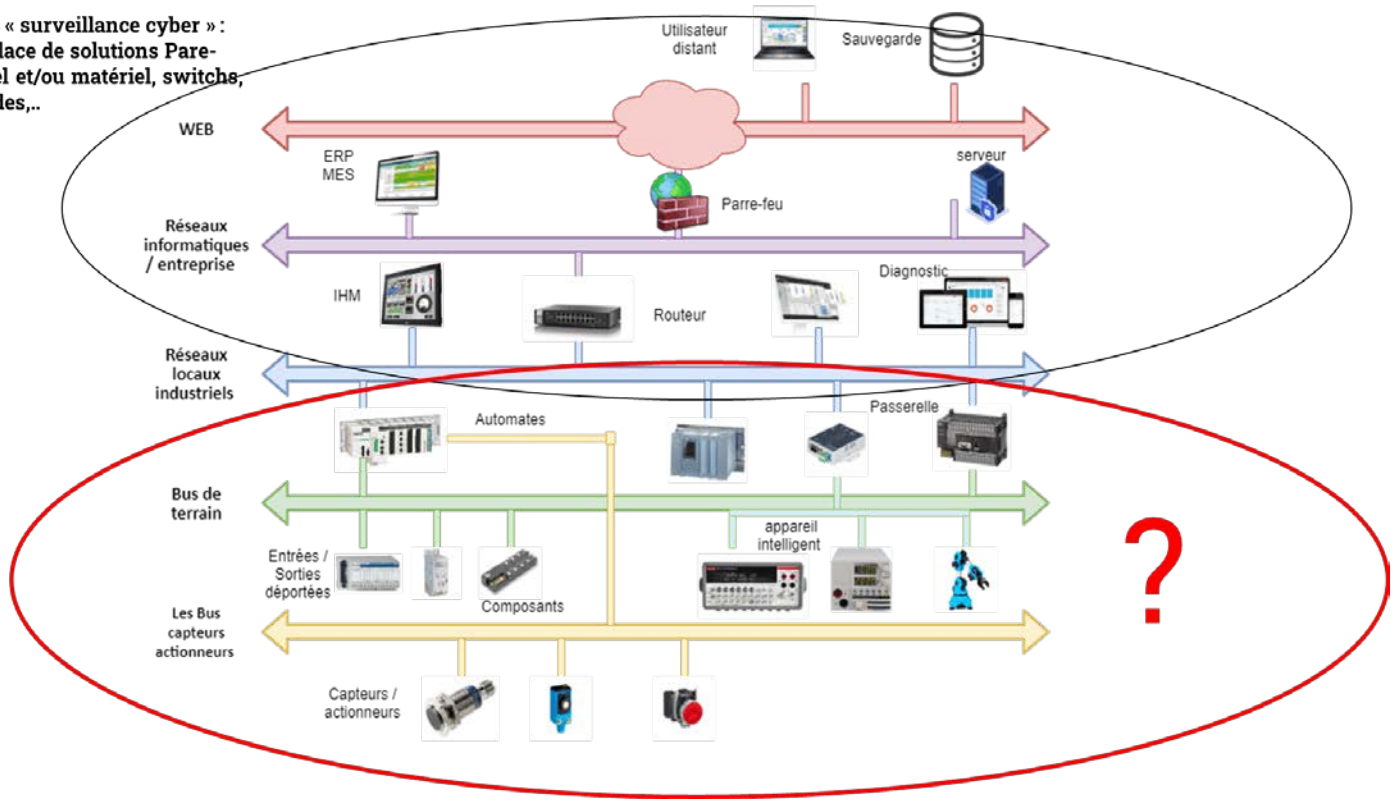
- *Utiliser un outil automatisé d'analyse statique : L'utilisation d'un logiciel d'analyse statique permet d'automatiser la vérification des règles du standard MISRA.*
- *Faire des audits de code source de façon ponctuelle*

- Mise en place d'outils **d'analyse de code** (statique)

L´analyse statique de code correspond à une analyse du logiciel réalisée sans exécuter le programme.
Les outils d'analyse de code statique peuvent analyser les versions de code source pour trouver des failles sémantiques et de sécurité. Ils peuvent mettre en évidence le code problématique par nom de fichier, emplacement et numéro de ligne de l'extrait de code concerné.
*Ils permettent également de s´assurer que le code est écrit selon des **règles de programmations** définis, comme par exemple les règles **MISRA-C**.*

Attention à l'effet « TITANIC » !

Zone sous « surveillance cyber » : Mise en place de solutions Pare-feu logiciel et/ou matériel, switchs, VPN, sondes,..



Contact

Jean-Christophe MARPEAU
Ingénieur-conseil / Référent Cybersécurité
✆ 06 07 73 66 34
marpeau@captronic.fr

www.captronic.fr