SECURE
Cyber Resilience for SMEs

Exigences essentielles en matière de cybersécurité de la législation sur la cyber-résilience (CRA): Annexe I, Partie I

20/10/2025

Funded by
the European Union

Déclaration de financement de l'UE : Financé par l'Union européenne sous le numéro GA n° 101190325.
Les points de vue et opinions exprimés ne reflètent toutefois que celles de l'auteur ou des auteurs et ne reflètent pas nécessairement celles de l'Union européenne ou du Centre européen de compétences pour la cybersécurité industrielle, technologique et de recherche. Ni l'Union européenne ni l'autorité qui octroie le financement ne peuvent en être tenues responsables.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Avertissement de l'ECCC : Le projet est soutenu par le Centre européen de compétences en matière de cybersécurité et ses membres.

AVERTISSEMENT

Ce document fait partie du livrable D4.1 « Lignes directrices et ressources pour la conformité des SME à la législation sur la cyber-résilience (CRA) » du projet SECURE.

Le présent document est une traduction du guide original rédigé en anglais. Les abréviations sont conservées en anglais, telles qu'elles figurent dans la liste des abréviations.

Premier auteur : *Centre pour la cybersécurité Belgique (CCB)*

Deuxième auteur : *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Table des matières

Liste des tableaux et figures

Abréviations

API – Interface de programmation d'application (Application Programming Interface)

APT – Menaces persistantes avancées (Advanced Persistent Threats)

BSIMM – Modèle de maturité pour la sécurité des systèmes d'information (Building Security in Maturity Model)

CI/CD – Intégration continue et livraison/déploiement continus (Continuous Integrations and Delivery/Deployment)

CRA – Loi sur la cyber-résilience (Cyber Resilience Act)

CVD – Divulgation coordonnée des vulnérabilités (Coordinated Vulnerability Disclosure)

CVE – Vulnérabilités et expositions courantes (Common Vulnerabilities and Exposures)

CVSS – Système commun de notation des vulnérabilités (Common Vulnerability Scoring System)

DAST – Tests dynamiques de sécurité des applications (Dynamic Application Security Testing)

DoS – Déni de service (Denial of Service)

DREAD – Dégâts, Reproductibilité, Exploitabilité, Utilisateurs affectés et Découvrabilité (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability**)**

ENISA – Agence de l'Union européenne pour la cybersécurité (European Union Agency for Cybersecurity)

EOL – Fin de vie (End of life)

EPSS – Système de notation de prédiction des exploits (Exploit Prediction Scoring System)

ETSI – Institut européen des normes techniques (European Technical Standards Institute)

EU – Union européenne (European Union)

FIRST VCMM – Modèle de maturité de coordination des vulnérabilités FIRST (FIRST Vulnerability Coordination Maturity Model)

GDPR – Règlement général sur la protection des données (General Data Protection Regulation)

HTTPS/TLS – Protocole hypertexte sécurisé/Sécurité de la couche transport (Hyper Text Protocol Secure/Transport Layer Security)

ICS – Système de contrôle industriel (Industrail Control System)

IEC – Commission électrotechnique internationale (International Electrotechnical Commission)

IoT – Internet des objets (Internet of Things)

IPSec – Protocole de sécurité Internet (Internet Protocol Security)

ISO – Organisation internationale de normalisation (International Standards Organisation)

JTAG – Groupe d'action conjoint pour les tests (Joint Test Action Group)

LINDDUN – Liaison, identification, non-répudiation, détection, divulgation de données, ignorance et non-conformité (Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness and Non-compliance)

MFA – Authentification multifactorielle (Multi-factor authentication)

MITRE ATT&CK – Tactiques, techniques et connaissances communes des adversaires (Adversarial Tactics, Techniques and Common Knowledge)

MQTT – Transport de télémétrie par mise en file d'attente de messages (Message Queuing Telemetry Transport)

NIST – Institut national des normes et technologies (États-Unis) (National Institute of Standards and Technology)

NIST SSDF – Cadre de développement logiciel sécurisé du NIST (NIST Secure Software Development Framework)

NTIA – Administration nationale des télécommunications et de l'information (États-Unis) (National Telecommunications and Information Administration)

OPENSSF VEX – Fondation pour la sécurité open source – Échange sur l'exploitabilité des vulnérabilités (Open-Source Security Foundation Vulnerability Exploitability eXchange)

OS – Système d'exploitation (Operating System)

OTA – A distance (Over The Air)

OWASP – Projet mondial ouvert sur la sécurité des applications (Open Worldwide Application Security Project)

OWASP ASVS – Norme de vérification de la sécurité des applications OWASP (OWASP Application Security Verification Standard)

OWASP SAMM – Modèle de maturité de l'assurance logicielle OWASP (OWASP Software Assurance Maturity Model)

PDE – Produit avec éléments numériques (Product with Digital Elements)

PSIRT – Équipe d'intervention en cas d'incident de sécurité des produits (Product Security Incident Response Team)

SAST – Test statique de sécurité des applications (Static Application Security Testing)

SBOM – Nomenclature logicielle (Software Bill of Materials)

SCA – Analyse de la composition logicielle (Software Composition Analysis)

SIEM – Gestion des informations et des événements de sécurité (Security Information and Event Management)

SME – Petite et moyenne entreprise (Small and Medium Enterprise)

SOC – Centre des opérations de sécurité (Security Operations Centre)

SQL – Langage de requête structuré (Structured Query Language)

SSDLC – Cycle de vie sécurisé du développement logiciel (Secure Software Development Lifecycle)

SSL – Secure Sockets Layer (Secure Sockets Layer)

STRIDE – Usurpation d'identité, falsification, répudiation, divulgation d'informations, déni de service, élévation de privilèges (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)

TPM – Module de plateforme sécurisée (Trusted Platform Module)

UART – Récepteur-émetteur asynchrone universel (Universal Asynchronous Receiver-Transmitter)

USB – Bus série universel (Universal Serial Bus)

VPN – Réseau privé virtuel (Virtual Private Network)

Introduction

Afin de se conformer à la **loi sur la cyber-résilience** (CRA), le règlement (UE) 2024/2847, en tant que fabricant, le CRA stipule une multitude d'exigences et d'obligations. L'une des principales exigences est que vous devez vous assurer que le produit comportant des éléments numériques (PDE) que vous mettez sur le marché « a été conçu, développé et produit conformément aux exigences essentielles en matière de cybersécurité énoncées dans la partie I de l'annexe I »[1] . L'annexe I comprend deux parties : la partie I porte sur les exigences en matière de cybersécurité relatives aux propriétés du produit, et la partie II traite des exigences en matière de gestion des vulnérabilités. La partie I comprend deux points, dont le premier stipule que

> *« Les produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques»*[2] .

Le point 2 précise les exigences auxquelles vos produits doivent se conformer.

Ce guide, élaborée dans le cadre **du projet SECURE**[3] dans le but de **soutenir les petites et moyennes entreprises (SME)**, approfondit les deux points de la partie I de l'annexe I, en fournissant **des suggestions pratiques et techniques non exhaustives, des exemples et des approches pour vous aider à vous conformer à chaque exigence**. Il est important de noter que toute référence à des normes, outils et cadres existants est purement **suggestive** et vise à rendre les exigences du CRA aussi concrètes que possible. Les recommandations formulées sont basées sur les meilleures pratiques reconnues et les approches courantes. Les outils mentionnés dans ce guide et la ligne directrice elle-même seront mis à jour à mesure que l'élaboration des normes spécifiques du CRA et les mesures d'exécution de la Commission européenne progresseront tout au long de la période d'adaptation de 2024 à 2027.

[1] Art. 13(1), CRA.

[2] Annexe I, partie I, paragraphe 1, CRA.

[3] Le projet « Renforcer la cyber-résilience des SME de l'UE » (SECURE) offre un soutien financier et des conseils aux SME pour se conformer à la CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Exigences essentielles de la législation sur la cyber-résilience (CRA): Annexe I, Partie I

1. Approche de la cybersécurité fondée sur les risques

Le point 1 de l'annexe I, partie I, stipule que

> *« Les produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques»*[4] .

Ce point est central dans le CRA et repose sur le principe de «sécurité dès la conception et par défaut». En substance, cela signifie que vous devez développer une **approche de cybersécurité fondée sur les risques** pour votre produit. Cette adaptation fondée sur les risques doit être défendable, documentée et proportionnée. Considérez la conformité au CRA comme un « parcours traçable » :

contexte du produit → risque → contrôles → preuve

La justification de ce parcours doit être soigneusement documentée dans la documentation technique obligatoire[5] , essentielle pour la conformité et l'auditabilité.

Dans la pratique, les fabricants doivent :

1. Évaluer les risques liés à la cybersécurité associés au PDE tout au long de son cycle de vie ;
2. Adapter les mesures de sécurité au niveau de risque (par exemple, un thermostat intelligent par rapport à un système de contrôle industriel) ;
3. Prendre en compte les modèles de menaces, les surfaces d'attaque et l'impact potentiel sur les utilisateurs et les systèmes.

Une première étape cruciale dans votre conformité au CRA consiste donc à effectuer une **évaluation des risques** pour votre PDE. Ce chapitre explore la manière de mener une telle évaluation des risques en présentant les approches possibles et en proposant des suggestions techniques.

Avant d'entrer dans les détails, un aperçu de deux pages sur les bases de l'évaluation des risques est fourni ci-dessous pour vous rafraîchir la mémoire. Ces éléments sont repris de manière plus détaillée dans le premier chapitre de ce guide, que nous vous recommandons de consulter. Toutefois, à des fins d'accessibilité, le résumé simplifié présente la manière dont les évaluations des risques sont généralement abordées[6] .

[4] Annexe I, partie I(1), CRA.

[5] Art. 31, CRA.

[6] Il est essentiel de noter que les orientations officielles sur la manière de mener l'évaluation des risques pour la CRA doivent encore être élaborées par la Commission européenne. Les orientations fournies ici résument

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Évaluation des risques 101

Lors de la réalisation d'une évaluation des risques, **six étapes** peuvent être envisagées :

1) Identification des **actifs** et **des menaces** = *identifier chaque actif (ce qui doit être protégé) en fonction de son exposition à une menace (ce qui pourrait mal tourner) ;*
2) Évaluation des **vulnérabilités** = *évaluer les vulnérabilités* ;
3) Prise en compte et évaluation des **impacts** et **des probabilités** = *représenter graphiquement les impacts et les probabilités des vulnérabilités → cela résulte en des « risques » spécifiques* ;
4) **Analyse** et **acceptation** des risques = *représenter graphiquement chaque risque et examiner votre niveau d'acceptation afin de hiérarchiser vos actions ;*

En plus de cette évaluation des risques, deux étapes finales sont nécessaires :

5) Mise en œuvre de **mesures d'atténuation** = *sélectionner et appliquer des contrôles de sécurité pour chaque risque ;*
6) Surveillance et réévaluation = *surveiller les menaces et les risques à chaque étape du cycle de vie des PDE et maintenir l'évaluation des risques à jour.*

Pour **les étapes 1 à 3**, vous pouvez élaborer une **matrice** qui vous permet de classer chaque menace, vulnérabilité et impact en fonction d'un certain niveau de risque et d'une certaine note. Pour ce faire, vous devez d'abord définir ce que chaque niveau (et chaque note) signifie pour vous à l'aide de tableaux descriptifs[7] .

- Faible
- Faible-moyen
- Moyen
- Moyen-élevé
- Élevé

Tableau 1 :
Exemple de matrice

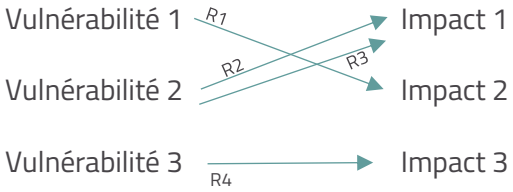
Risque/Menace	Menace 1	Menace 2	Score
Élevé			10
Moyen-élevé			
Moyen			
Faible Moyen			
Faible			0

[7] Par exemple, en ce qui concerne la survenue d'une menace, un niveau « faible » pourrait signifier une menace pouvant survenir une fois tous les dix ans, tandis qu'un niveau « élevé » pourrait signifier une menace pouvant survenir une fois par semaine. Vous devez disposer de tableaux descriptifs distincts pour les menaces, les vulnérabilités et les impacts, ainsi que pour les risques, ces derniers permettant de définir votre niveau d'acceptation.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

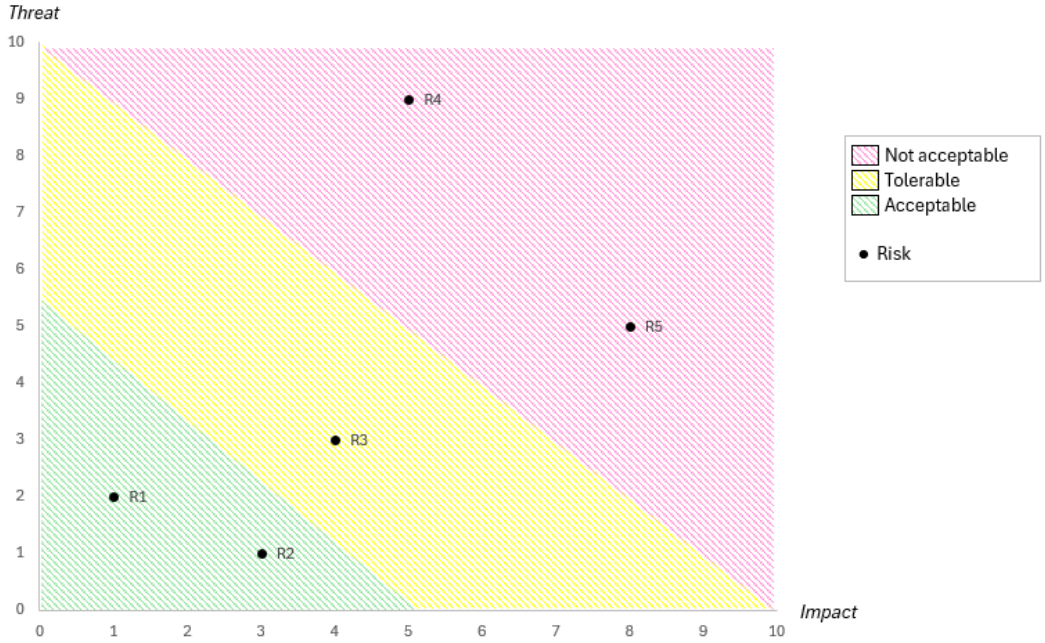
En établissant un lien entre les vulnérabilités et les impacts, vous pouvez ensuite visualiser les différents risques (R) :

Figure1 :
Visualisation des risques



Pour **la quatrième étape**, il est important de répertorier les risques rencontrés et de définir votre niveau d'acceptation de ces risques. Cela se fait souvent à l'aide d'un code couleur, par exemple :

Figure 2 :
Graphique d'acceptation des risques



Cela vous permet de hiérarchiser les mesures à prendre et d'élaborer des mesures d'atténuation et des contrôles de sécurité pour chaque risque afin de réduire les risques résiduels à un niveau acceptable.

Comme indiqué précédemment, ces éléments de l'évaluation des risques sont traités plus en détail ci-dessous (chapitre 1 du présent guide) à l'aide d'exemples et d'outils et de cadres recommandés pour vous aider.

1.1. Évaluation des risques liés à la cybersécurité tout au long du cycle de vie

Étant donné que les risques liés à la cybersécurité associés à votre PDE doivent être évalués tout au long du cycle de vie du produit, la réalisation d'une **évaluation des risques liés à la cybersécurité**

tout au long du cycle de vie implique **d'identifier, d'analyser et d'atténuer les risques liés à la cybersécurité** à chaque étape du cycle de vie d'un produit :

1. Conception
2. Développement
3. Production
4. Déploiement
5. Exploitation et maintenance
6. Fin de vie (EOL)

L'évaluation des risques doit être mise à jour en permanence tout au long de la « période de support »[8] , soit une période d'au moins cinq ans (ou, si la durée de vie du produit est inférieure à cinq ans, au moins jusqu'à la fin de la durée de vie du produit).

1.1.1. Étapes clés de l'évaluation des risques liés au cycle de vie

Lors de la réalisation de l'évaluation des risques, six étapes peuvent être envisagées, chacune d'entre elles étant précisée dans le tableau 2 ci-dessous.

Tableau 2 :
Étapes clés de l'évaluation des risques liés au cycle de vie

Étape clé	Clarification et suggestions
1. Identifier les actifs et les menaces	Distinguer entre : • Actifs : qu'est-ce qui doit être protégé ? Par exemple, micrologiciels, données utilisateur, canaux de communication. • Menaces : qu'est-ce qui pourrait mal tourner ? Par exemple, injection de logiciels malveillants, accès non autorisé.
2. Analysez les vulnérabilités	Utiliser des outils tels que : • Analyse statique du code ;

[8] Art. 13(8), CRA : La période d'assistance doit être déterminée par le fabricant, en tenant compte de la durée d'utilisation prévue du produit, des attentes des utilisateurs, de la nature (de la finalité) du produit et du droit de l'Union.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	• Analyse de la composition logicielle (SCA) ; • Tests de pénétration ; • Modélisation des menaces[9] (par exemple STRIDE, DREAD). Remarque : CVSS et STRIDE peuvent être utilisés conjointement dans un processus de modélisation des menaces. STRIDE peut aider à identifier les menaces potentielles, puis CVSS peut être utilisé pour évaluer la gravité des vulnérabilités liées à ces menaces, ce qui permet de mieux hiérarchiser les efforts d'atténuation[10] .
3. Évaluer l'impact et la probabilité des risques	Utiliser une matrice des risques pour établir des priorités en fonction : • L'impact (par exemple, violation de données, défaillance du système) ; • Probabilité (par exemple, exploitation connue, surface d'attaque).
4. Analysez les risques et leur acceptabilité	Définissez votre niveau d'acceptation et cartographiez vos risques en fonction de la menace et de l'impact afin de classer et de hiérarchiser vos actions.
5. Mettez en œuvre des mesures d'atténuation	Appliquez des contrôles de sécurité : par exemple, cryptage, authentification, démarrage sécurisé.
6. Surveiller et réévaluer	Surveillez en permanence les nouvelles menaces et mettez à jour les évaluations des risques en conséquence.

[9] La modélisation des menaces est abordée plus en détail au point 1.3.1.

[10] Le CVSS évalue la gravité des vulnérabilités, tandis que le risque tient également compte de l'impact commercial et de la probabilité.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.2. Cas d'utilisation par étape du cycle de vie

Afin de rendre l'évaluation des risques liés au cycle de vie plus concrète, le tableau 3 ci-dessous présente un aperçu des cas d'utilisation, y compris un exemple de risque et une stratégie d'atténuation, par étape du cycle de vie.

Tableau 3 :
Cas d'utilisation par étape du cycle de vie

Étape du cycle de vie	Cas d'utilisation	Risque	atténuation
Conception	Caméra domestique intelligente	Accès non autorisé aux flux vidéo	Mise en œuvre d'un chiffrement de bout en bout et paramètres de sécurité par défaut
Développement	Micrologiciel de l'appareil	Vulnérabilité liée au débordement de la mémoire tampon	Utiliser des pratiques de codage sécurisées et un scan automatisé des vulnérabilités
Production	Passerelle IoT industrielle	Compromission pendant la fabrication	Sécurisez la chaîne d'approvisionnement et la racine de confiance matérielle, utilisez des scellés inviolables d' t assurez un approvisionnement sécurisé
Déploiement	Routeur grand public	Identifiants par défaut inchangés	Changement de mot de passe obligatoire lors de la première utilisation
Exploitation et maintenance	Véhicule connecté	Vulnérabilités logicielles non corrigées	Mises à jour OTA avec contrôles d'intégrité
Fin de vie	Thermostat intelligent	Appareil abandonné avec micrologiciel exploitable	Fournir des instructions de mise hors service sécurisées et d'effacement des données, une politique de mise à jour de sécurité en fin de vie et

			l'exportation des données pour les utilisateurs

1.1.3. Outils et cadres pour vous aider

La liste ci-dessous présente plusieurs outils et cadres qui peuvent vous aider, bien qu'une liste plus exhaustive et des normes harmonisées soient encore en cours d'élaboration.

- ISO/IEC 27005 – Gestion des risques
- NIST SP 800-30 – Méthodologie d'évaluation des risques
- ENISA Threat Landscape – Informations actualisées sur les menaces
- OWASP ASVS – Vérification de la sécurité des applications
- Modèle STRIDE
- Modèle d'évaluation des risques DREAD
- LINDDUN
- CVSS

1.2. Mesures de sécurité adaptées

La deuxième dimension d'une approche de la cybersécurité fondée sur les risques consiste à adapter les mesures de sécurité au niveau de risque. Cette adaptation doit être proportionnée aux risques identifiés dans l'annexe I, partie I(1). Expliquons ce que cela signifie à l'aide de six étapes claires, de principes et de deux exemples de produits : un thermostat intelligent (risque faible à modéré) et un système de contrôle industriel (ICS) (risque élevé).

1.2.1. Effectuer une classification des risques du produit

Lors de l'évaluation des risques spécifiques à un produit, il est important de prendre en compte les dimensions suivantes.

- **Exposition aux menaces** : le produit est-il
  - Connecté à Internet ?
  - Largement déployé ?
  - Destiné au grand public ?

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Utilisation prévue vs utilisation abusive raisonnablement prévisible ?

- **Impact d'une compromission** : quel serait l'impact sur la sécurité, les pertes financières, la confidentialité, les infrastructures critiques ?
- **Attrait de l'attaque :** serait-elle un tremplin pour un mouvement latéral ?
- **Profil de l'utilisateur :** consommateur, SME, opérateur d'infrastructure critique ?

Sur la base de ces considérations, le produit peut être classé comme présentant un risque faible acceptable, un risque modéré tolérable ou un risque élevé inacceptable[11] .

1.2.2. Définir les objectifs de sécurité par niveau de risque

Le tableau 4 illustre comment les objectifs de sécurité peuvent ensuite être adaptés au niveau de risque du produit précédemment établi.

Tableau 4 :
Objectifs de sécurité par niveau de risque

Niveau de risque	Objectifs de sécurité
Faible (par exemple, thermostat intelligent)	• Empêcher toute exploitation insignifiante ; • Garantir la confidentialité ; • Maintenir la capacité de mise à jour.
Modéré	• Détecter et atténuer les vecteurs d'attaque connus ; • Appliquer l'authentification ; • Sécuriser les communications.
Élevé (par exemple, ICS)	• Renforcement de la sécurité ; • Défense en profondeur ; • Confiance dans la chaîne d'approvisionnement ; • Démarrage sécurisé ; • Surveillance des incidents.

[11] Cela vous oblige à définir à l'avance comment noter ces éléments à l'aide d'une matrice et comment les notes correspondent aux niveaux de risque. Pour une classification plus précise, cinq niveaux de risque peuvent être pris en compte au lieu de trois : risque faible, moyen-faible, moyen, moyen-élevé, élevé.

1.2.3. Adapter les exigences essentielles du CRA au niveau de risque

Selon le niveau de risque, les exigences essentielles du CRA peuvent avoir différentes applications pratiques. Le tableau 5 illustre cela pour les niveaux de risque faible et élevé et les exemples de produits correspondants, à savoir le thermostat intelligent et l'ICS.

Tableau 5 :
Exigences essentielles du CRA par niveau de risque

Exigences du CRA	Risque faible	Risque élevé
Sécurité dès la conception et par défaut	Désactiver les ports de débogage ; paramètres par défaut robustes	Nomenclature complète des composants logiciels (SBOM[12]) ; démarrage sécurisé ; système d'exploitation renforcé
Gestion des vulnérabilités	Politique publique en matière de CVD ; security.txt ; surveillance de la boîte de réception ; mécanisme de correctifs	Divulgation coordonnée ; PSIRT ; réponse rapide
Journalisation et surveillance	Journaux d'événements locaux	Journalisation à distance ; intégration SIEM
Contrôle d'accès	Authentification par code PIN ou application	Accès basé sur les rôles ; MFA ; privilège minimal
Mécanisme de mise à jour	Mises à jour OTA avec le consentement de l'utilisateur	Mises à jour signées ; restauration sans risque
Protection contre les accès non autorisés	Règles de pare-feu de base	Systèmes de détection d'intrusion hôte ; contrôles d'intégrité du micrologiciel

[12] La SBOM est précisée plus en détail à la section 4.1.

1.2.4. Utilisation de la modélisation des menaces pour affiner les mesures

Pour la modélisation des menaces, les méthodes STRIDE, LINDDUN ou les arbres d'attaque peuvent être utilisées pour valider l'adéquation des contrôles.

Pour les exemples de produits, cela signifie :

- **Thermostat intelligent** : se concentrer sur l'usurpation d'identité, la falsification et le déni de service ;
- **ICS** : couvrir toutes les menaces STRIDE et les menaces persistantes avancées (APT).

1.2.5. Sélectionner les contrôles par niveau de risque

Le tableau 6 propose différents contrôles par domaine de sécurité pour les exemples pratiques, le thermostat intelligent (risque faible) et l'ICS (risque élevé).

Tableau 6 :
Contrôles par niveau de risque

Domaine de sécurité	Risque faible	Risque élevé
Authentification	Authentification par application ; modification du mot de passe par défaut	MFA ; contrôle d'accès basé sur un certificat
Sécurité du micrologiciel	Micrologiciel signé ; mises à jour OTA ; restauration à sécurité intégrée	Démarrage sécurisé ; intégration TPM ; assurance de la chaîne d'approvisionnement
Communication	HTTPS/TLS	VPN ; IPSec ; segmentation du réseau ; zéro confiance
Surveillance	Rotation de base des journaux	Journalisation en temps réel ; détection des anomalies ; intégration SOC ; journaux synchronisés dans le temps
Interface utilisateur	Panneau de configuration simple	Console d'administration détaillée ; fonctionnalités de piste d'audit

1.2.6. Preuves de conformité des documents

Comme indiqué précédemment, un élément clé de la conformité avec l'ARC consiste à documenter au minimum les preuves suivantes :

- Justification de la classification des risques ;
- Décisions de contrôle liées aux risques ;
- Résultats des tests et de la validation ;
- Politiques de mise à jour et de gestion des vulnérabilités ;
- Alignement du cycle de vie du développement sécurisé (par exemple, ISO/IEC 27034, IEC 62443-4-1) ;
- Matrice de traçabilité reliant les risques -> contrôles -> tests de vérification -> preuves (à conserver dans la documentation technique)

1.2.7. Exemples

Le tableau 7 fournit des exemples supplémentaires de mesures de mise en œuvre pour les cas pratiques à faible et à haut risque.

Tableau 7 :
Mesures de mise en œuvre par niveau de risque

Produit	Thermostat intelligent	ICS
Considérations relatives aux risques	• Connecté à Internet, contrôle le chauffage dans les maisons privées ; • Sensibles à la vie privée, mais faible impact sur la sécurité ou l'économie.	• Utilisé dans des infrastructures critiques (par exemple, traitement de l'eau) ; • Impact élevé sur la sécurité et le fonctionnement.
Classification des risques	Risque faible	Risque élevé

Mesures de mise en œuvre	• Modifier le mot de passe par défaut lors de la première utilisation ; • Communication HTTPS avec le backend ; • Mises à jour du micrologiciel signées ; • Enregistrement local uniquement[13] ; • Formulaire de contact de base pour signaler les vulnérabilités.	• Matériel sécurisé dès la conception avec TPM ; • Démarrage sécurisé et mises à jour signées avec possibilité de restauration ; • Accès basé sur les rôles et authentification multifactorielle ; • Segmentation du réseau et règles de pare-feu ; • Enregistrement dans le SIEM central ; • SBOM complet à chaque mise à jour ; • Processus coordonné de divulgation des vulnérabilités (CVD)

1.3. Prise en compte des modèles de menaces, des surfaces d'attaque et de l'impact potentiel sur les utilisateurs et les systèmes

Le CRA met l'accent sur une approche de la cybersécurité fondée sur les risques. Comme indiqué ci-dessus, cela signifie que les fabricants doivent adapter leurs mesures de sécurité aux menaces réelles, aux points d'exposition et aux conséquences potentielles pour les utilisateurs et les systèmes. Il ne s'agit pas d'une directive creuse, mais d'un appel à une approche fondée et adaptée au contexte. Pour mettre en œuvre efficacement cette obligation, trois concepts clés doivent être pris en compte conjointement : les modèles de menace, les surfaces d'attaque et l'analyse d'impact, qui constituent la troisième et dernière dimension de l'approche de la cybersécurité fondée sur les risques. Examinons ces éléments un par un et voyons comment ils s'articulent entre eux.

[13] À noter : les journaux locaux réduisent la valeur forensic, l'exportation facultative avec le consentement de l'utilisateur est recommandée.

1.3.1. Modèles de menace : qui attaque, pourquoi et comment ?

La modélisation des menaces est un processus structuré qui consiste à identifier qui pourrait attaquer votre produit, comment et pour quelle raison. Pensez aux script kiddies, aux cybercriminels organisés ou même aux acteurs étatiques. Leurs motivations varient, allant du gain financier au sabotage ou à l'espionnage, et leurs compétences vont du niveau basique au niveau avancé.

Pour structurer cela, vous pouvez utiliser des méthodes telles que :

- STRIDE ;
- MITRE ATT&CK pour les techniques d'attaque connues ;
- LINDDUN pour les menaces liées à la confidentialité ;
- les arbres d'attaque ou les chaînes de cyber-destruction pour cartographier les chemins d'attaque.

Pour revenir aux exemples pratiques, cela signifie :

- **Thermostat intelligent** : les menaces se limitent souvent à des voisins curieux ou à des attaques aléatoires, où quelqu'un pourrait manipuler les réglages de température ou la consommation d'énergie ;
- **ICS** (par exemple, dans une station d'épuration) : les menaces sont fondamentalement différentes, par exemple, des groupes APT ou des gangs de ransomware tentent de saboter des processus physiques ou de fermer une entreprise.

Le résultat de la modélisation des menaces est une liste claire d'objectifs de sécurité spécifiques au produit et à son environnement.

1.3.2 Surfaces d'attaque : par où un attaquant peut-il s'introduire ?

Une surface d'attaque est l'ensemble des points à partir desquels un attaquant peut interagir avec le système ou l'influencer. Plus il y a d'interfaces et de points d'accès, plus le risque est grand.

Les surfaces d'attaque typiques sont les suivantes :

- Les interfaces réseau telles que Wi-Fi, Bluetooth, MQTT ou HTTP ;
- Les interfaces locales telles que USB, UART, JTAG (pour le débogage) ;
- Les mécanismes de mise à jour tels que les mises à jour OTA ou USB ;
- API, applications mobiles, tableaux de bord cloud ;
- Composants externes provenant de la chaîne d'approvisionnement.

L'analyse de ces surfaces implique de vérifier quels composants sont inutilement exposés, quels services sont activés mais inutiles, et si l'accès est correctement protégé. Idéalement, vous devriez limiter la surface d'attaque en :

- Appliquant des principes de sécurité tels que l'exposition minimale, les paramètres par défaut sécurisés et le renforcement ;
- Désactivant les ports ou services inutilisés ;
- l'authentification et le chiffrement à chaque interface.

Appliqué aux exemples, cela signifie :

- **Thermostat intelligent** : utilise généralement le Wi-Fi et éventuellement le Bluetooth, avec une simple connexion au cloud - Les interfaces de débogage peuvent être ouvertes pendant les tests et doivent être désactivées en production ;
- **Passerelle ICS** : sera physiquement protégée, avec des mises à jour USB blindées, des réseaux segmentés et aucune interface externe.

Il est donc essentiel de cartographier minutieusement la surface d'attaque afin de savoir où la sécurité est réellement nécessaire.

1.3.3 Analyse d'impact : que se passe-t-il si les choses tournent mal ?

La dernière étape consiste à déterminer l'impact potentiel d'une attaque réussie. Le CRA exige que les mesures de sécurité soient proportionnées à cet impact. Cela inclut non seulement les dommages techniques, mais aussi :

- les dangers pour l'utilisateur (par exemple, blessures dues au contrôle de la température) ;
- la violation de la vie privée (par exemple, déduction des habitudes de vie à partir des données du thermostat) ;
- la perte de disponibilité ou de continuité des activités (par exemple, fermeture d'une usine) ;
- la responsabilité juridique (par exemple, violation du CRA ou du GDPR) ;
- atteinte à la réputation et risque de marché.

L'impact doit être pris en compte à plusieurs niveaux :

- Utilisateur : d'un inconvénient mineur à des situations mettant la vie en danger ;

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Organisation : augmentation de la charge de travail du service d'assistance à interruption d'activité ;
- Société : des bugs innocents aux menaces pesant sur les infrastructures critiques.

Là encore, la proportionnalité est essentielle : un robot jouet ne nécessite pas le même niveau de sécurité qu'une pompe médicale.

1.3.4 Intégration : de l'analyse aux mesures

Lorsque ces trois éléments constitutifs sont réunis (modèle de menace, surface d'attaque et impact), une base solide est créée pour adapter les mesures de sécurité.

Une approche type se présente comme suit :

1. Définir l'utilisation et le contexte du produit ;
2. Réaliser une modélisation des menaces pour comprendre les acteurs, leurs motivations et les voies d'attaque ;
3. Cartographier la surface d'attaque et identifier les vulnérabilités ;
4. Analyser l'impact sur les utilisateurs, les organisations et la société ;
5. Sélectionner les mesures en fonction du risque (risque = probabilité × impact) ;
6. Documentez tout pour vous conformer aux exigences de l'ARC et aux audits.

Concrètement, cela signifie :

- **Thermostat intelligent** : cryptage, politique de mots de passe forts, mises à jour OTA signées et déclaration de confidentialité simple.
- **Passerelle ICS** : démarrage sécurisé, racine de confiance matérielle, réseaux segmentés, journalisation SIEM, gestion des rôles et SBOM complète avec surveillance des vulnérabilités.

2. Conception et développement sécurisés

Pour revenir au point 1 de l'annexe I, partie I, du CRA, l'approche de la cybersécurité fondée sur les risques et l'adaptation repose sur le principe de « sécurité dès la conception et par défaut », c'est-à-dire que les PDE doivent être conçus et développés de manière à être sécurisés dès le départ. Il ne suffit plus d'ajouter la sécurité comme une couche optionnelle après coup ; elle doit faire partie intégrante de l'ensemble du processus de développement du produit.
La « sécurité dès la conception », la « sécurité par défaut » et l'utilisation de pratiques de développement sécurisées constituent le cœur d'une stratégie de produits numériques résilients.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Elles garantissent que la sécurité n'est pas une réflexion après coup, mais une partie intégrante et démontrable du produit, exactement comme l'exige le CRA.

En utilisant des normes internationales telles que les directives IEC 62443, ISO 27034, OWASP et ENISA, les fabricants peuvent appliquer efficacement ces principes tout en respectant leurs obligations de conformité.

Les produits doivent être :

1. **Sécurisés dès leur conception** : la sécurité est intégrée dès les premières étapes du développement ;
2. **Sécurisés par défaut** : les paramètres par défaut doivent donner la priorité à la sécurité (par exemple, mots de passe forts, ports ouverts minimaux, etc.)
3. **Développés de manière sécurisée** : en utilisant des pratiques de codage sécurisées et la modélisation des menaces.

2.1. Sécurité dès la conception – Sécurisé dès la conception initiale

« Sécurisé dès la conception » signifie que la cybersécurité est prise en compte dès la phase de conception dans les décisions relatives à l'architecture, au choix des composants et à l'interaction entre les sous-systèmes. La sécurité doit être aussi fondamentale que la fonctionnalité ou la convivialité.

Exemple pratique :

Lors de la conception d'un module de serrure intelligente, les décisions suivantes sont prises immédiatement :

- Appliquer un chiffrement de bout en bout entre l'application et la serrure ;
- Stocker les clés en toute sécurité dans un TPM ou un élément sécurisé ;
- Désactiver physiquement les ports de débogage après la production.

Les normes et directives pertinentes à cet égard sont les suivantes :

- IEC 62443-4-1 : exige l'intégration de la sécurité dans le cycle de vie des logiciels ;
- ISO/IEC 27034 : sécurité des applications dans le cycle de vie du développement logiciel ;
- NIST SP 800-218 SSDF ;
- ENISA Bonnes pratiques en matière de développement de logiciels sécurisés.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.2. Sécurité par défaut – Sécurité sans configuration utilisateur

« Sécurité par défaut » signifie que les produits sont livrés avec la configuration la plus sécurisée en standard. L'utilisateur ne doit pas avoir à deviner si la sécurité est activée. La sécurité est la base, et non un « paramètre avancé » facultatif.

Exemples de paramètres de sécurité par défaut :

- Pas de paramètres par défaut partagés, imposer la configuration des identifiants lors du premier démarrage ou l'appairage sans mot de passe avec des facteurs sécurisés ;
- Seuls les ports réseau nécessaires sont ouverts (principe d'exposition minimale) ;
- Mises à jour du micrologiciel signées et vérifiées par défaut ;
- Journalisation et piste d'audit activées par défaut pour les fonctions critiques.

Les directives pertinentes à cet égard comprennent :

- OWASP Secure Configuration : meilleures pratiques pour des paramètres par défaut sécurisés ;
- NIST SP 800-128 : Guide pour une gestion de la configuration axée sur la sécurité.

2.3. Pratiques de codage sécurisé

L'ARC exige que le développement de logiciels soit effectué conformément à des pratiques de développement sécurisées éprouvées et en accordant une attention constante aux menaces. Cela signifie, entre autres :

Codage sécurisé :

- Validation des entrées (contre les injections SQL, les débordements de tampon, etc.) ;
- Utilisation de bibliothèques sécurisées et de cryptage ;
- Tests de robustesse et analyse statique du code.

Modélisation des menaces :
Pour chaque composant du logiciel, les éléments suivants doivent être évalués :

- Qui pourrait attaquer ce composant ?
- Comment pourrait-il le faire ?
- Quel serait l'impact ?

Des cadres tels que STRIDE (Microsoft), OWASP Threat Dragon et MITRE ATT&CK peuvent aider à identifier systématiquement les vulnérabilités et les voies d'attaque.

Les normes et directives pertinentes à cet égard comprennent :

- Liste de contrôle des pratiques de codage sécurisé de l'OWASP ;
- ISO/IEC 27001 Annexe A.14 : Exigences de sécurité dans le développement ;
- Directives de l'ENISA sur la modélisation des menaces (2022) ;
- BSI TR-03161 (Allemagne) : Développement de logiciels sécurisés.

2.4. Concrètement pour les fabricants

En résumé, une organisation qui souhaite développer des PDE conformes à la norme CRA doit :

- Adopter un cycle de vie de développement logiciel sécurisé (SSDLC), tel que décrit dans la norme CEI 62443-4-1 ou NIST SP 800-218 SSDF ;
- Disposer d'une politique de révision et de test du code axée sur les vulnérabilités (SAST, DAST, fuzzing) ;
- Appliquer systématiquement la modélisation des menaces à chaque composant important ;
- Fournir des produits avec des ports fermés standard, la journalisation activée et des ports d'accès sécurisés ;
- Adopter une fonction PSIRT avec des rôles clairs et des processus d'astreinte ;
- Définir des portes de qualité de sécurité dans CI/CD (SAST, DAST, SCA, analyse des secrets) avec des politiques de rejet de la construction.

3. Gestion de la sécurité tout au long du cycle de vie

Au-delà de la conception, du développement et de la production sécurisés des PDE, votre produit doit également rester sécurisé tout au long de son cycle de vie. Les produits numériques évoluent, et leur sécurité doit en faire autant. Cela signifie que la sécurité doit être gérée et prise en compte en permanence, même après la mise sur le marché du PDE.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Concrètement, les fabricants sont tenus de gérer[14] :

1. Surveiller en permanence les vulnérabilités ;
2. Fournir des mises à jour et des correctifs de sécurité en temps opportun ;
3. Maintenir une politique de divulgation des vulnérabilités et communiquer les risques de manière transparente aux utilisateurs et aux régulateurs.

3.1. Surveillance continue des vulnérabilités

Une fois qu'un produit est commercialisé, les fabricants doivent continuer à détecter activement et systématiquement les vulnérabilités. Cela implique notamment :

- Surveiller les bases de données sur les vulnérabilités, telles que la base de données européenne sur les vulnérabilités[15] ;
- Surveiller les avis des fournisseurs ;
- le suivi des vulnérabilités et expositions courantes (CVE) liées aux composants ou bibliothèques utilisés ;
- l'utilisation de SBOM pour identifier et suivre les dépendances ;
- surveiller en interne les nouvelles vulnérabilités grâce à des programmes de prime aux bogues, des tests de pénétration ou des audits de sécurité.

Exemple :

Un fabricant de caméras réseau utilise des modules de micrologiciels open source. La base de données CVE révèle que l'un de ces modules contient une vulnérabilité critique (par exemple CVE-2023-XXXXX). Le fabricant est tenu de surveiller et d'évaluer cette information et, le cas échéant, de prendre les mesures appropriées.
Les sources pertinentes à cet égard sont notamment les suivantes :

- CVE ;
- EPSS (Exploit Prediction Scoring System) ;
- Directives de l'ENISA en matière de gestion des vulnérabilités ;
- ISO/IEC 30111 : Processus de gestion des vulnérabilités.

[14] Bien que les exigences en matière de gestion des vulnérabilités soient traitées en détail dans l'annexe I, partie II, elles découlent des points 1 et 2 de l'annexe I, partie I, et sont donc déjà abordées dans la présente ligne directrice.
[15] Art. 17(5), CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3.2. Mises à jour de sécurité et correctifs en temps opportun

Le CRA exige des fabricants qu'ils réagissent rapidement aux vulnérabilités connues et qu'ils distribuent gratuitement et efficacement des mises à jour de sécurité pendant toute la période de support.

Ces mises à jour doivent :

- Être signées numériquement et validées ;
- Disposer d'un mécanisme de restauration à sécurité intégrée ;
- être installables automatiquement avec des options de désactivation et/ou avec une interaction minimale de l'utilisateur ;
- Rester disponibles pendant au moins 10 ans après leur publication ou pendant le reste de la période de support (selon la période la plus longue).

Exemple :

Un fabricant de thermostats intelligents découvre une vulnérabilité dans la pile Wi-Fi. En deux semaines, un correctif de sécurité est développé, testé et distribué via une mise à jour OTA signée. Les utilisateurs reçoivent une notification claire et la mise à jour est automatiquement installée au redémarrage de l'appareil.

Les sources pertinentes à cet égard sont les suivantes :

- ISO/IEC 29147 : Divulgation coordonnée des vulnérabilités ;
- NIST SP 800-40 : Guide de gestion des correctifs en entreprise ;
- ETSI EN 303 645 : Base de référence en matière de sécurité pour l'IoT grand public (y compris les mécanismes de mise à jour des logiciels).

3.3. Politique de signalement des vulnérabilités et de communication transparente

La transparence est essentielle. Le CRA exige des fabricants qu'ils :

- Publient une politique de divulgation coordonnée des vulnérabilités ;
- Fournir un point de contact (par exemple, security@company.eu) pour les signalements ;

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Informer rapidement les utilisateurs et les autorités telles que l'ENISA ou l'autorité nationale de surveillance en cas de risques graves ;
- Communiquent de manière transparente sur les correctifs disponibles, les mesures d'atténuation et les risques résiduels.

Exemple :

Un hacker éthique signale une vulnérabilité critique dans un système d'alarme connecté via la plateforme publique CVD du fabricant. Dans les 72 heures, la réception est confirmée et, après analyse interne, l'ENISA est informée via la plateforme unique de signalement de l'ENISA (points de contact nationaux). Un correctif est déployé dans les trois semaines et tous les utilisateurs sont informés du risque et de la solution par e-mail et par des notifications sur l'application.

Les sources pertinentes à cet égard sont notamment les suivantes :

- FIRST Vulnerability Coordination Maturity Model (VCMM) ;
- ISO/IEC 29147 : Lignes directrices pour la divulgation des vulnérabilités ;
- Lignes directrices de l'ENISA pour la divulgation coordonnée des vulnérabilités (2022) ;
- OpenSSF VEX (Vulnerability Exploitability eXchange).

4. Sécurité de la chaîne d'approvisionnement

Le CRA reconnaît qu'un produit n'est jamais totalement « indépendant » : il se compose de dizaines, voire de centaines de composants provenant de fournisseurs externes, de projets open source et de partenaires matériels. C'est pourquoi le CRA fixe des exigences explicites pour la gestion des risques liés à la cybersécurité au sein de la chaîne d'approvisionnement.

Dans la pratique, les fabricants doivent :

1. Maintenir une vue d'ensemble actualisée et transparente des composants logiciels utilisés via un SBOM ;
2. Exiger des fournisseurs qu'ils se conforment à la sécurité conforme avec le CRA ;
3. Surveiller et gérer activement les risques associés aux dépendances open source et externes.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.1. Nomenclature logicielle (SBOM)

Une SBOM est similaire à une liste d'ingrédients pour les logiciels : elle contient un aperçu de tous les composants, versions et origines des éléments logiciels utilisés, y compris les bibliothèques open source.

Le CRA exige des fabricants qu'ils tiennent à jour une SBOM et qu'ils soient en mesure de la soumettre aux régulateurs et aux autorités sur demande. La publication de la SBOM pour les utilisateurs est facultative[16] . Cette SBOM sert de base pour :

- L'analyse des vulnérabilités (par exemple via le suivi CVE) ;
- L'évaluation de l'impact en cas de zero-days ;
- Audits de la chaîne d'approvisionnement.

Exemple :

Un fabricant de routeurs intelligents établit une SBOM qui indique clairement que le produit utilise :

- OpenSSL 1.1.1n ;
- BusyBox 1.35.0 ;
- Une version modifiée d'un module pare-feu open source.

Lorsqu'une vulnérabilité dans OpenSSL (CVE-2022-XXXX) est divulguée, le fabricant peut immédiatement vérifier si le produit est concerné et réagir de manière appropriée.

Les sources pertinentes à cet égard sont notamment les suivantes :

- CycloneDX, SPDX : formats SBOM (également recommandés par l'ENISA et la NTIA) ;
- ISO/IEC 5230 (OpenChain) : conformité des logiciels de la chaîne d'approvisionnement ;
- Outils OpenSSF pour la génération de SBOM et la détection des vulnérabilités.

4.2. Exigences de sécurité pour les fournisseurs

Le CRA exige également des fabricants qu'ils s'assurent que leurs fournisseurs et développeurs externes respectent des exigences de sécurité comparables à celles de leur propre équipe. La

[16] Si elles sont mises à la disposition des utilisateurs, précisez où et comment ceux-ci peuvent y accéder.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

responsabilité ne peut être transférée ; les vulnérabilités des composants tiers peuvent également entraîner des obligations de conformité au CRA.

Concrètement, cela signifie :

- L'inclusion de clauses de cybersécurité dans les contrats avec les fournisseurs ;
- La réalisation d'une vérification préalable de la sécurité lors de la sélection des fournisseurs de logiciels ;
- Vérification périodique de la conformité des partenaires, par exemple :
    - ISO/IEC 27001 (sécurité de l'information) ;
    - IEC 62443-4-1 (développement de produits sécurisés) ;
    - les modèles de maturité OWASP SAMM ou BSIMM.
- Droits d'audit contractuels et niveaux d'assurance minimaux (par exemple, certification des déclarations de conformité) pour les composants critiques ;
- Notification dans les 24 heures des vulnérabilités critiques découvertes par les fournisseurs et affectant vos PDE.

Exemple :

Un fabricant d'appareils médicaux IoT travaille avec un fournisseur de logiciels en Asie. Le contrat stipule que ce fournisseur :

- Développe de manière sécurisée conformément à la norme CEI 62443-4-1 ;
- Documente tous les composants open source utilisés ;
- Maintienne une politique de vulnérabilité avec obligation de signalement dans les 24 heures.

4.3. Gestion des risques liés aux bibliothèques open source et externes

Les logiciels open source offrent de nombreux avantages, mais comportent également des risques : vulnérabilités, mises à jour manquantes, licences peu claires ou responsables de maintenance peu fiables. Le CRA exige des fabricants qu'ils gèrent et surveillent activement ces risques.

Les meilleures pratiques comprennent :

- Utiliser des scanners de dépendances (par exemple OWASP Dependency-Check, Snyk, Trivy) ;

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Alertes automatiques en cas de vulnérabilités (par exemple via GitHub Advisories) ;
- N'utilisez que des projets open source maintenus et matures ;
- Appliquez des barrières de sécurité dans les pipelines CI/CD (en bloquant les builds présentant des CVE connus) ;
- Utilisez VEX pour réduire le bruit provenant des CVE non exploitables ;
- Exigez une réactivité minimale de la part des responsables de la maintenance lors de la sélection des logiciels libres.

Exemple :

Un fabricant utilise une bibliothèque JavaScript populaire (par exemple Log4j) dans une interface web. Après avoir découvert Log4Shell (CVE-2021-44228), le fabricant sait exactement quelles versions sont concernées grâce à l'analyse SBOM et peut segmenter et corriger les produits concernés.

Les sources pertinentes à cet égard sont les suivantes :

- NIST SSDF (Secure Software Development Framework) ;
- ENISA OSS Security Guidelines ;
- OpenSSF Scorecard : évaluation objective de la qualité des projets open source.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusion

Ce guide présente une première **traduction technique des exigences de l'annexe I, partie I, du CRA en suggestions et recommandations pratiques**. Elles mettent en évidence **quatre éléments** essentiels à votre conformité avec le CRA : (1) une approche de la cybersécurité fondée sur les risques, qui implique une évaluation des risques, des mesures de sécurité adaptées et la prise en compte des modèles de menaces, des surfaces d'attaque et des impacts ; (2) le principe de sécurité dès la conception/par défaut ; (3) les obligations en matière de gestion de la sécurité tout au long du cycle de vie de votre PDE ; (4) les considérations et contrôles relatifs à la chaîne d'approvisionnement. Pour chaque élément, **des suggestions pratiques** sont formulées sur la manière de mettre en œuvre et de respecter ces obligations, sur la base des meilleures pratiques et normes reconnues. Celles-ci sont toutefois susceptibles d'être modifiées en fonction des discussions en cours sur les normes actuelles et de l'évolution de la réglementation. Comme prochaines étapes pour les SME, il est recommandé de consulter les lignes directrices supplémentaires disponibles dans le **référentiel** SECURE, telles que **le cadre méthodologique d'évaluation de la conformité au CRA** pour obtenir une boîte à outils étape par étape et une liste de contrôle sur la conformité au CRA au-delà de l'annexe I, ainsi que **CRA 101 : Comprendre les obligations de la CRA** pour obtenir un aperçu condensé et accessible aux débutants de vos obligations légales en vertu du CRA.