RED ALERT LABS
IoT Security

CyberPass Alliance

AI-powered CRA/RED Supervision and Compliance Hub

Résumé du projet

CyberPass-Alliance est une plateforme européenne reposant sur l'intelligence artificielle et issue de la solution CyberPass développée par Red Alert Labs. Son objectif est de permettre aux autorités de surveillance nationales et des Etats Membres (ANFR, ANSSI, douanes, MSAs, CSIRTs, NCCs) ainsi qu'aux acteurs économiques (fabricants, importateurs, distributeurs, Organismes Notifiés) de gérer le cycle de vie complet de la conformité CRA/RED, tout en automatisant la détection, la classification et le reporting des non-conformités et vulnérabilités liées au CRA/RED, en facilitant la supervision et la coopération transfrontalière via l'IA, des connecteurs et des dashboards interopérables..

La plateforme automatise la classification des produits à risque, la gestion des non-conformités et la coopération transfrontalière. Elle réduit drastiquement le coût, le besoin d'expertise et le temps de traitement pour les autorités comme pour les entreprises, en créant un véritable hub de confiance européen.

Objectifs

- Renforcer la capacité des autorités (EUPCN, Adcos, NCCAs, ANFR, ANSSI, MSAs, CSIRTs, NCCs) à détecter en continu les produits suspects en non-conformité CRA/RED (incluant Art. 3.3 d/e/f du RED).
- Fournir et partager des informations européennes consolidées sur la conformité et les vulnérabilités, enrichies par IA et interopérables avec ICSMS, Safety Gate, EUCC et Cyber Hubs, afin de renforcer la coopération transfrontalière.
- Automatiser la gestion du cycle de conformité CRA/RED côté fabricants et opérateurs.
- Contribuer à la certification et standardisation européenne des produits connectés incluants les produits IA sécurisées.

Red Alert Labs (S.A.S)
Société par actions simplifiée
827 677 303 R.C.S. Créteil

3 rue Parmentier
94140 Alfortville
France

www.redalertlabs.com

RED ALERT LABS
IoT Security

Cas d'usages intégrés

Autorités de surveillance (Adcos, ANFR, douanes, MSAs)

- Liste automatisée de produits connectés suspects, priorisation des contrôles, vérification CRA/RED Art. 3.3.
- Valeur ajoutée CyberPass : IA de classification des risques, workflow de non-conformités, dashboard autorité.

ANSSI / NCCA/ NCC-FR

- Vue consolidée des produits certifiés/non-conformes, génération automatique de rapports supervision (CRA Art. 19).
- Valeur ajoutée CyberPass : Connecteurs EUCC/ICSMS, IA scoring de non-conformité, reporting automatisé.

Coopération transfrontalière (MSAs UE, Cyber Hubs)

- Partage d'informations anonymisées, coordination via ICSMS + Safety Gate, campagnes de contrôle ciblées.
- Valeur ajoutée CyberPass : IA pour stratégie d'échantillonnage, dashboard européen interopérable.

Manufacturers & opérateurs économiques

- Détection/notification de vulnérabilités, génération automatique DoC/Annexe IV, échanges directs avec MSAs.
- Valeur ajoutée CyberPass : Automatisation DoC, liaison autorité, dashboard produits (statut conformité).

Vulnerability lifecycle (CRA Art. 11)

- Analyse d'impact sur le niveau d'assurance/conformité, triage IA, déduplication et priorisation.
- Valeur ajoutée CyberPass : Mapping CRA/standards EN, intégration CVE/CVSS, dashboard conformité Art. 11.

Positionnement différenciateur

- End-to-end CRA compliance lifecycle : évaluation → surveillance continue → incident de non-conformité → enforcement.
- AI augmentation : génération rapports, triage impacts de vulnérabilités, scoring conformité.
- Réduction des coûts pour autorités & PME grâce à l'automatisation.
- Trust layer européen : CyberPass comme hub neutre entre fabricants, autorités, NBs et Commission.

Structure projet (36 mois)

WP1 – Coordination & conformité légale

- Pilotage du projet et gestion administrative.
- Cadre *compliance by design* (privacy, security, CRA/RED by design).
- Suivi qualité, éthique, et gouvernance (advisory board).

WP2 – IA pour détection & classification de non-conformités

- Détection d'anomalies sur produits connectés (SBOM, doc technique).
- Classification de produits suspects/non conformes au CRA/RED (incluant Art. 3.3 d/e/f).
- Scoring IA de probabilité de non-conformité et génération de rapports automatisés.

WP3 – Portail & services Autorités (ANFR, ANSSI, MSAs, NCCAs, CSIRTs)

- Dashboard autorité pour suivi des produits, priorisation des contrôles et escalades.
- Connecteurs vers EUCC, ICSMS, Safety Gate.
- Rapports supervision automatisés (CRA Art. 19).
- Campagnes de contrôle coordonnées avec partage d'informations transfrontalières.

WP4 – Portail & services Fabricants, NB, Opérateurs économiques

- Automatisation de la génération DoC et Annexe IV.
- Gestion des actions correctives et notifications directes aux MSAs.
- Intégration cycle de vie vulnérabilités (CRA Art. 11) : triage IA, déduplication, analyse d'impact.
- Dashboard de conformité produit en temps réel.

WP5 – Coopération transfrontalière & interopérabilité européenne

- Partage d'informations anonymisées entre autorités via ICSMS + Safety Gate.
- Dashboard européen interopérable pour MSAs et Cyber Hubs.
- IA pour stratégie d'échantillonnage et campagnes de contrôle ciblées.
- Tests réels avec ANFR, ANSSI, 2–3 MSAs UE, 3 fabricants IoT, et 3 NB.

WP6 – Standardisation, certification & dissémination

- Contribution aux schémas de certification européens (EUCC, AI sécurisée, CRA).
- Ateliers, formations (Campus Cyber, EU events) et diffusion des résultats.
- Publications et positionnement dans la normalisation (ENISA/ECCC, CEN/CENELEC).
- Visibilité internationale et transfert vers le marché.

KPIs (indicateurs clés)

- **≥ 60 % de réduction du délai de détection des non-conformités** (impact direct pour les autorités).
- **≥ 40 % des vulnérabilités détectées automatiquement par IA** (preuve d'innovation technologique).
- **≥ 50 % d'automatisation des tâches CRA/RED côté fabricants et organismes notifiés** (gain de productivité et baisse de coût).
- **≥ 30 % de gain de temps** pour les autorités de surveillances dans le traitement des non-conformités (efficience publique).
- **≥ 20 produits IoT analysés en conditions réelles** (preuve de mise en œuvre et scalabilité).
- **≥ 5 autorités nationales intégrées** (dont… ???, ANFR ?, ANSSI ?, MSAs UE, CSIRTs) (preuve d'adoption européenne).
- **≥ 3 campagnes pilotes transfrontalières coordonnées** via ICSMS/Safety Gate (impact coopération UE).
- **≥ 1 schéma de certification européen contribué** (EUCC/CRA ou IA sécurisée) (impact réglementaire et standardisation).