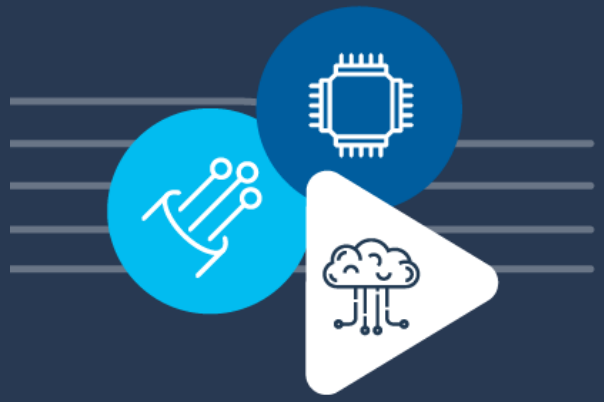


SuppliersDay
INFRABEL

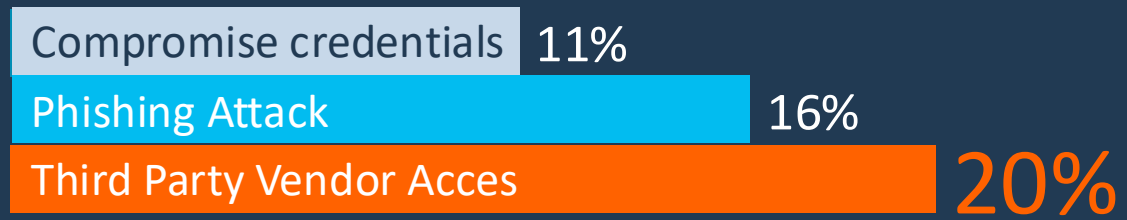
ICT


LIVE
TOUT LE TRAFFIC
EST INTERROMPU.
AUCUN TRAIN
NE CIRCULE.
Quai
Gpeer
11
BREAKING NEWS
CYBER ATTACK ON BELGIAN RAILWAYS
07:57
ALL TRAINS STOP DUE TO CYBERATTACK ON SIGNALING SYSTEMS

Pourquoi nous comptons sur *vous* pour *notre* Cyber-Résilience

Principaux vecteurs 2025

32%
des cyberattaques ont exploité des failles logicielles non corrigées



17x
Les attaques visant la Supply Chain coûtent désormais 17 fois plus cher à résoudre que les violations directes (au sein même de l'entreprise).

+ 1 semaine
72% des entreprises mettent plus d'une semaine à rétablir pleinement leurs activités. Dans les secteurs où les enjeux sont importants, les délais de reprise dépassent souvent six semaines.

20 à 80 mia €
Les pertes se sont élevées à environ 20 à 80 milliards € en seulement 15 mois à la suite de violations de données majeures.

Un cadre legal et normatif

Loi NIS2

Infrabel est une Entité Essentielle au regard de la Loi NIS2

Cyber Resilience Act

Tous les produits digitaux achetés par Infrabel doivent être conformes aux exigences du CRA

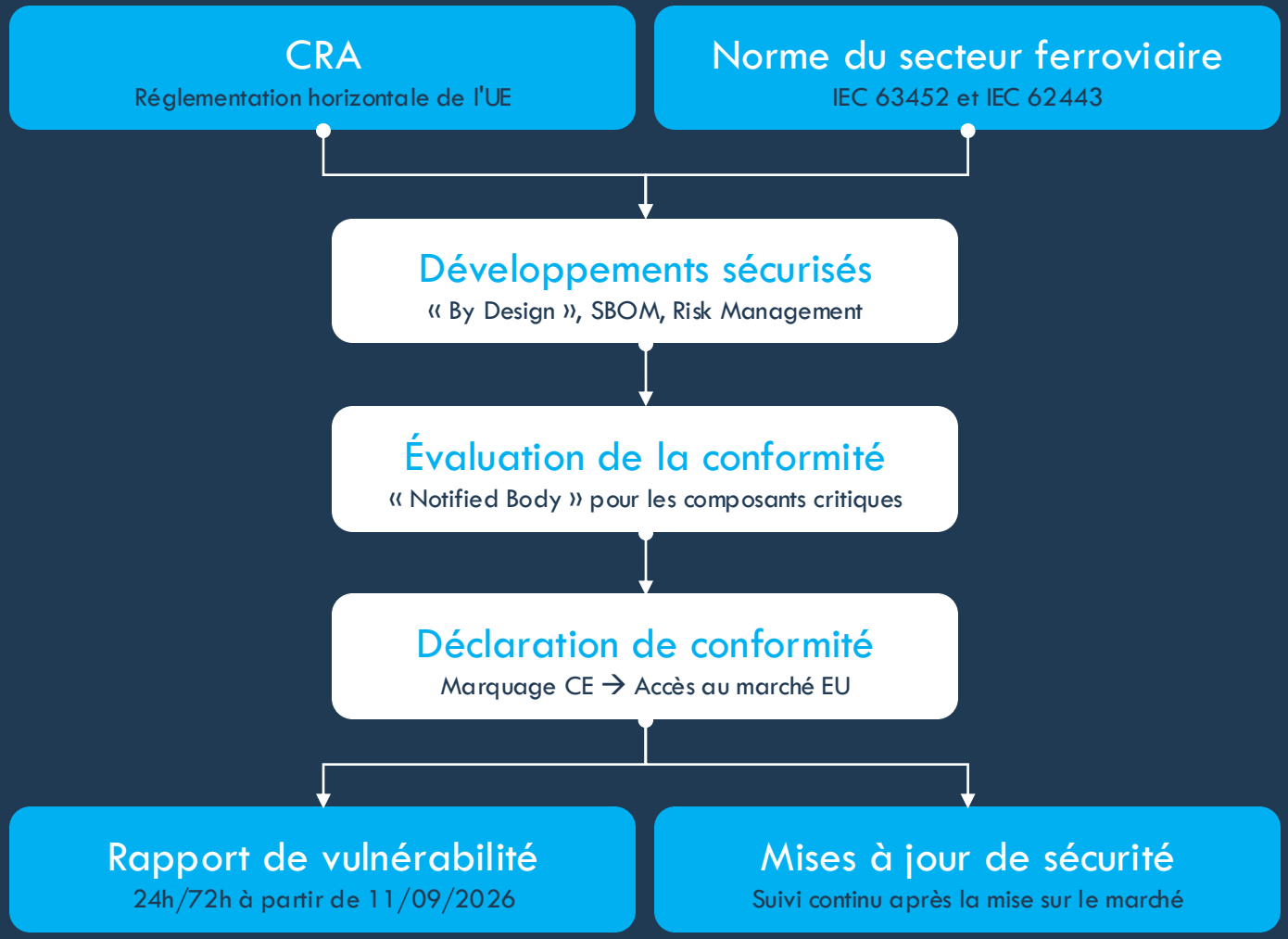
IEC 62443 // 63452

Respecter les normes Industrielles et sectorielles est essentielles pour les solutions critiques

AI Act

Se conformer à l'AI Act est devenu une obligation

L’impact du CRA



Le **CRA ne remplace pas** ce que nous faisons déjà dans le cadre des normes IEC 63452 et IEC 62443 ou des spécifications de Cybersécurité existantes.

Le **CRA vient s'ajouter** à ces référentiels, et c'est précisément cette traçabilité totale entre la législation horizontale et les normes sectorielles que les autorités de régulation attendent de nous.

Qu’entendons-nous de vous concrètement ?

1. Culture de la cybersécurité et formation du personnel
2. Gouvernance de la Cybersécurité et gestion des risques
3. Cyber- Sécurité dès la conception et gestion des vulnérabilités
4. Surveillance continue, détection active et réponse aux incidents
5. Cybersécurité de la chaîne d’approvisionnement et des tiers
6. Engagement, clauses contractuelles et gestion des responsabilités

Nos défis

Le modernisation des solutions digitales ferroviaires

Dans les **10 prochaines** années, Infrabel va moderniser ses solutions digitales (FRMRS, New Signaling/IXL, etc). Mais**, la Cyber-Résilience, c'est déjà aujourd'hui.**

Souveraineté digitale, technologique et stratégique

Infrabel, en tant qu'infrastructure ferroviaire critique, doit **garantir sa souveraineté face aux risques** digitaux et liés à sa Supply Chain.

Pourquoi nous comptons sur vous pour deployer des solutions basées sur l'Intelligence Artificielle

L’Intelligence Artificielle, ami ou ennemi ?

Selon le rapport « Global Cybersecurity Outlook 2026 » du Forum Economique Mondial, l'intelligence artificielle devrait être le **principal moteur du changement** dans le domaine de la cybersécurité, et ce dès les prochains mois.

L'IA chez Infrabel : opportunité stratégique, exigences nouvelles

L'IA s'impose dans tous nos métiers — mais en infrastructure ferroviaire critique, **un système mal conçu, biaisé ou mal encadré met en jeu la sécurité, la conformité et la confiance**.

Opportunités stratégiques

- Maintenance prédictive
- Optimisation du trafic et gestion des incidents
- Détection d'anomalies
- Aide à la décision opérationnelle

Responsabilités nouvelles

- AI Act (UE 2024/1689) — transports classés **haut risque**
- Sanctions **considérables** (AI Act)
- ISO 42001 — référence de maturité IA
- Souveraineté des données et explicabilité exigées

Un cadre légal et normatif

AI Act

Conformité obligatoire
pour tout système IA livré à Infrabel

RGPD

Encadrement strict
des données personnelles et évaluations d'impact

Souveraineté

Hébergement et traitement
en juridiction européenne voire dans nos DCs

ISO 42001

Référence
pour évaluer la maturité IA des fournisseurs

Qu'attendons-nous de vous concrètement ?

Deux axes complémentaires : Gouvernance IA & Projets IA

1. **Conformité AI Act** : marquage CE et documentation technique
2. **ISO 42001** : politique IA, gestion des risques, certification
3. **Éthique & IA responsable** : xAI, supervision humaine, formation

AI

4. **IA digne de confiance** : explicabilité, robustesse, validation
5. **Sécurité by Design** : tests adversariaux, pipelines sécurisés
6. **Souveraineté & IP** : données en UE, propriété des modèles

Réalisation de projets intégrant l'IA

Exigences techniques pour des projets IA sûrs, conformes et durables

1 Trustworthy AI

- Supervision humaine — “human in the loop”
- Robustesse et précision en conditions réalistes
- Explicabilité — xAI fortement recommandé

2 Security by Design

- Tests adversariaux pour systèmes critiques
- Pipelines de données sécurisés et tracés
- Surveillance continue & alertes

3 Data Governance

- Souveraineté — juridiction européenne
- Propriété intellectuelle des modèles
- Conformité RGPD

4 Lifecycle & Maintenance

- Documentation technique complète
- Versioning, traçabilité, rollback possible
- Notification des vulnérabilités, gestion fin de vie

Trois messages-clés essentiels

Conformité non négociable

L'AI Act n'est pas une option. Anticiper dès maintenant la mise en conformité de chaque système livré.

Gouvernance comme fondation

Conformité AI Act, ISO 42001, politiques IA, gestion des risques : condition sine qua non en ferroviaire critique.

Partenariat & confiance

Nous construisons des partenariats IA durables avec des fournisseurs engagés et matures.

“We may have all come on different ships, but we’re in the same boat now.”

-Martin Luther King Jr.-