Guide de la Cyber Résilience

à l'usage des Fournisseurs d'Infrabel

INFRABEL

Guide de la Cyber Résilience
à l'usage des Fournisseurs d'Infrabel

Sensibilisation et orientation en matière de cybersécurité et de cyber-résilience

Infrabel gère des infrastructures ferroviaires critiques
et doit respecter plusieurs cadres et normes de cybersécurité.

PRINCIPES CADRES & NORMES

- Loi CER
- Loi NIS2
- Cyber Resilience Act
- Directive RED
- ISO 27001
- CyFun
- NIST CSF
- IEC 62443 / IEC 63452

VOS OBLIGATIONS EN TANT QUE FOURNISSEUR

Gestion des Risques
Évaluer et réduire
les vulnérabilités

Protection des Données
Sécuriser vos systèmes
et informations

Détection & Réponse
Surveiller et réagir
aux incidents

Cycle de Vie
Maintenir la sécurité
tout au long du cycle

Assurez la continuité et la conformité de vos services !

INFRABEL

Table des matières

GUIDE DE LA CYBER RESILIENCE A L'USAGE DES FOURNISSEURS D'INFRABEL

Ce guide vise à sensibiliser et orienter les fournisseurs d'Infrabel sur les exigences concrètes en matière de cybersécurité et de cyber-résilience. Il s'agit de garantir que vos prestations, produits et services respectent les obligations légales et réglementaires actuelles, tout en protégeant la continuité des activités.

Infrabel, en tant que gestionnaire d'infrastructures ferroviaires critiques, doit se conformer à des cadres comme :

- la loi CER,
- la loi NIS2,
- le Cyber Resilience Act (CRA),
- la Radio Equipment Directive (RED),
- ainsi qu'à des normes et référentiels reconnus tels que
  - ISO 27001
  - cadre national CCB CyberFundamentals (CyFun)
  - NIST CSF
  - IEC 62443
  - et la future norme ferroviaire IEC 63452.

En tant que fournisseur, il vous est donc demandé d'adopter des mesures de sécurité robustes couvrant la gestion des risques, la protection de vos données et de vos services, la détection et la réponse aux incidents, sur l'ensemble du cycle de vie de vos produits ou services qu'Infrabel vous achète.

Un impératif légal et stratégique

La cybersécurité n'est plus optionnelle : des réglementations européennes comme NIS2 engagent directement la responsabilité des opérateurs critiques et de leurs fournisseurs, avec des contrôles et sanctions à la clé. La cyber-résilience est aussi essentielle pour garantir la continuité de votre activité et la confiance d'Infrabel.

Exigences concrètes et bonnes pratiques

Ce guide est structuré par domaines pratiques (gestion des accès, réponse aux incidents, sécurité des chaînes d'approvisionnement, etc.) et illustre pour chacun des mesures attendues, assorties d'exemples de bonnes pratiques éprouvées, notamment adaptées au contexte ferroviaire.

Alignement sur les standards reconnus

Les recommandations formulées ici s'appuient sur des référentiels internationaux (ISO/IEC 27001, NIST CSF v2.0, IEC 62443...) ainsi que sur le cadre national belge CyberFundamentals (CyFun). En les suivant, vous facilitez la démonstration de votre conformité et adoptez un langage commun avec Infrabel en matière de sécurité.

Panorama des cadres réglementaires et normatifs

Les exigences de cyber-résilience d'Infrabel envers ses fournisseurs découlent de plusieurs textes de loi belges, de directives européennes récentes et de normes de référence.

Le tableau ci-dessous en résume les principaux :

Cadre / Norme	Portée et rôle pour les fournisseurs
Critical Entities Resilience (CER)	Réglementation visant à renforcer la résilience et la sécurité des infrastructures essentielles en Europe face aux risques, qu'ils soient d'origine naturelle ou humaine. Elle impose aux opérateurs de secteurs critiques (transport, énergie, santé, etc.) des obligations de prévention, de gestion de crise et de continuité d'activité afin d'assurer la disponibilité et la fiabilité des services indispensables.
Directive NIS2	Réglementation imposant aux entités essentielles et importantes (transport, énergie, etc.) un socle minimal de mesures de cybersécurité. NIS2 exige notamment la gestion des risques, la surveillance des accès, le traitement des incidents, la sécurisation de la chaîne d'approvisionnement et la mise en place de plans de continuité. Les fournisseurs critiques d'Infrabel sont concernés de manière indirecte (et parfois directe s'ils relèvent eux-mêmes de NIS2), ils doivent appliquer des normes strictes équivalentes pour éviter de devenir le maillon faible.
Cyber Resilience Act (CRA)	Réglementation européenne (règlement 2024/2847) établissant des exigences de cybersécurité pour les produits avec éléments numériques (logiciels, objets connectés, équipements). Les fabricants et fournisseurs de tels produits devront dès 2026 démontrer une sécurité par conception (par ex. absence de vulnérabilités connues au moment de la mise sur le marché), la mise à jour régulière des correctifs de sécurité, ainsi qu'un processus formel de gestion des vulnérabilités et incidents (notification d'alerte sous 24 h, rapport détaillé sous 72 h en cas de faille exploitée). Exemple : si vous fournissez à Infrabel un logiciel ou équipement connecté, vous devrez disposer d'un processus de suivi des vulnérabilités et fournir des mises à jour de sécurité tout au long du cycle de vie du produit.
Directive RED	La directive UE 2014/53/UE (dite RED) régit les équipements radio. Un acte délégué y a introduit des exigences de cybersécurité applicables à

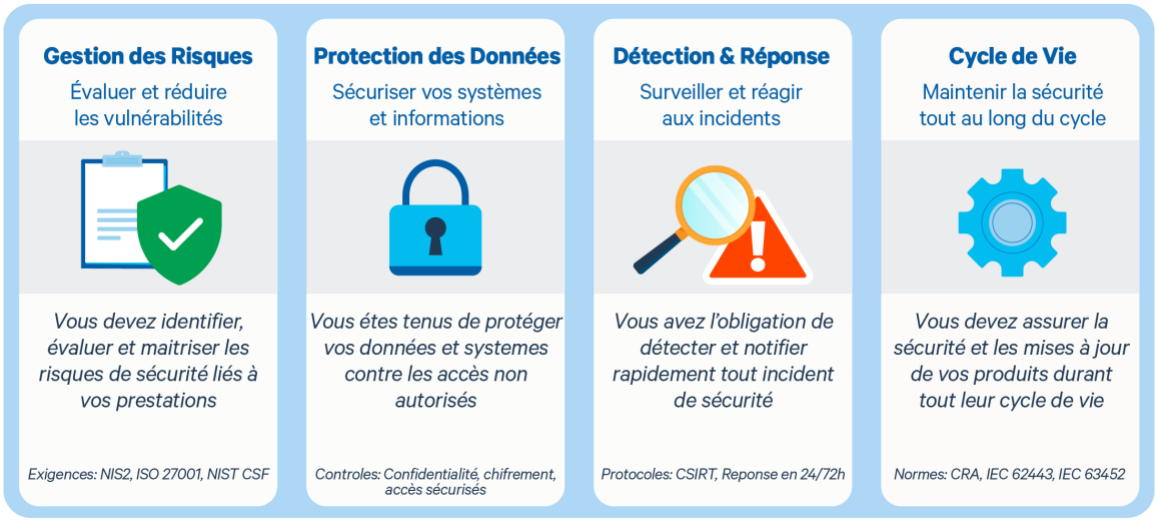
	certaines catégories d'appareils sans fil ou connectés (par ex. objets IoT grand public, modules radio industriels). En pratique, cela se traduit par l'implémentation de fonctions de sécurité telles que l'empêchement des accès non autorisés, la protection des données personnelles et de la vie privée, et la prévention des risques de fraude sur les équipements concernés. La conformité devra être prouvée via des standards techniques harmonisés (par ex. les nouvelles normes EN 303 645 et EN 18031-x inspirées d'IEC 62443). Exemple : si vous vendez à Infrabel un capteur sans fil pour l'infrastructure, il devra intégrer des contrôles de sécurité réseau et respecter ces normes.
ISO/IEC 27001:2022	Norme internationale de Système de Management de la Sécurité de l'Information (SMSI). Elle fournit un cadre complet de politiques, processus et contrôles pour gérer la sécurité des informations. Infrabel utilise l'ISO 27001 comme référence centrale de son propre ISMS. La transposition belge de NIS2 reconnaît d'ailleurs l'ISO 27001 (version 2022) comme équivalente au cadre CyFun pour démontrer la conformité aux exigences minimales. Une certification ISO 27001 de votre entreprise constituerait ainsi un gage fort de confiance.
CyberFundamentals (CyFun)	Cadre de cybersécurité défini par le Centre pour la Cybersécurité Belgique, conçu pour l'évaluation NIS2. Il décline des mesures de sécurité minimales en trois niveaux d'assurance (Basique, Important, Essentiel) proportionnés à la taille/criticité de l'organisation. Un fournisseur d'Infrabel peut être amené à se faire évaluer selon CyFun (ou à fournir une certification ISO 27001 équivalente) dans le cadre des contrôles périodiques de conformité imposés aux opérateurs essentiels en Belgique.
NIST Cybersecurity Framework 2.0	Référentiel volontaire de gestion des risques cyber, largement adopté internationalement. La version 2.0 du NIST CSF structure la sécurité en 6 fonctions : Gouverner, Identifier, Protéger, Détecter, Réagir, Récupérer, couvrant chacune plusieurs catégories de contrôles (ex. gestion des identités, protection des données, surveillance continue, réponse aux incidents, etc.). Ce vocabulaire commun est utilisé par Infrabel pour articuler sa stratégie de cybersécurité (axes Identify, Protect, Detect, Respond, Recover, Govern).

	S'aligner sur ces catégories facilite la communication et la couverture exhaustive des risques.
IEC 62443	Série de normes internationales spécialisées dans la sécurité des systèmes industriels et des SCADA/OT. Elles définissent à la fois des exigences techniques (ex. 7 Exigences Fondamentales d'IEC 62443-1-1 couvrant l'authentification, la protection des communications, l'intégrité, la disponibilité, la gestion des accès, etc.) et des processus de cycle de vie (ex. IEC 62443-4-1 pour le développement sécurisé, 62443-2-1 pour les programmes de gestion de sécurité industrielle). Pour les fournisseurs de solutions industrielles à Infrabel, l'IEC 62443 sert de cadre technique de référence aligné avec les obligations légales (les principes d'IEC 62443 sont en effet repris implicitement dans NIS2, CRA et RED).
AI Act	L'AI Act, règlement européen sur l'intelligence artificielle, introduit de nouvelles obligations pour les fournisseurs de solutions d'IA et leurs clients. Ce cadre impose une classification des systèmes d'IA selon leur niveau de risque, avec des exigences accrues pour les systèmes à haut risque (comme ceux utilisés dans la gestion des infrastructures critiques, la sécurité ou les transports). L'AI Act renforce le niveau d'exigence dans la relation fournisseur, obligeant à une collaboration étroite pour assurer la conformité, la sécurité et la gestion des risques liés à l'intelligence artificielle, tout en favorisant une approche proactive et transparente tout au long du cycle de vie des systèmes d'IA.
IEC 63452 **(à venir)**	Future norme internationale dédiée à la cybersécurité ferroviaire. Actuellement en cours de finalisation au sein du Comité TC9 de l'IEC, IEC 63452 adaptera les principes d'IEC 62443 aux spécificités des systèmes ferroviaires (signalisation, matériel roulant, systèmes au sol, etc.), en couvrant tout le cycle de vie (conception, exploitation, maintenance) et en définissant clairement les responsabilités des différents acteurs (exploitant, intégrateur, fournisseur, mainteneur). Avec une adoption attendue en Europe dès 2026, cette norme remplacera la spécification ferroviaire actuelle CLC/TS 50701 et deviendra le nouveau socle de conformité pour le secteur rail, en cohérence avec NIS2 et le CRA. Les fournisseurs intervenant sur des systèmes ferroviaires devront ainsi rapidement s'y conformer.

Chaque fournisseur d'Infrabel n'est pas forcément concerné par toutes ces normes et lois, mais vous devez identifier ceux qui s'appliquent à vos produits/services et à votre rôle.

Par exemple, un éditeur de logiciel ou fabricant d'objet connecté sera directement visé par le CRA et la RED, tandis qu'une société prestataire de maintenance système sera plus concernée par NIS2 et l'ISO 27001.

Quoi qu'il en soit, Infrabel attend de l'ensemble de ses partenaires une attitude proactive consistant à mettre en œuvre les mesures concrètes détaillées ci-après, qui synthétisent les exigences communes à ces référentiels.



Gouvernance de la sécurité et gestion des risques

Pourquoi ?

Une bonne gouvernance de la cybersécurité est la pierre angulaire d'une cyber-résilience efficace. Infrabel s'attend à ce que ses fournisseurs intègrent la sécurité de l'information dans leur management et adoptent une approche par les risques pour dimensionner des mesures de sécurité appropriées.

Ceci est non seulement une bonne pratique (conforme à l'esprit des normes ISO 27001 et NIST CSF), mais également une obligation légale implicite : NIS2 impose par exemple aux dirigeants d'entités critiques de superviser la gestion des risques cyber et de valider des plans de continuité d'activité.

Mesures attendues

Mesure attendues	Description
Politique de sécurité et responsabilités définies	Vous devez formellement nommer un responsable de la cybersécurité ou une équipe en charge de celle-ci, et disposer d'une politique de cybersécurité interne approuvée par votre direction. Cette politique doit couvrir vos principaux enjeux (confidentialité des données, disponibilité des systèmes, etc.) et se conformer aux lois en vigueur en Belgique et aux exigences d'Infrabel dans le cadre d'un contrat. Elle définit les rôles et responsabilités de chacun en matière de protection des informations. Exemple : une PME fournisseur a désigné un « CISO » en interne, une pratique encouragée par Infrabel.
Analyses de risques régulières	Adoptez un processus documenté d'évaluation des risques sur vos actifs et services, en particulier ceux liés au périmètre d'Infrabel. Avant tout nouveau projet ou contrat, identifiez les scénarios de menace pertinents, évaluez les impacts potentiels (y compris sur la sûreté ferroviaire le cas échéant) et sélectionnez des mesures de sécurité proportionnelles aux risques identifiés. Exemple : avant de connecter un système au réseau d'Infrabel, un fournisseur réalise une analyse de risques en utilisant la méthode EBIOS de l'ANSSI et conforme à IEC 62443-3-2 pour justifier le niveau de sécurité requis (SL 1, 2 ou plus) en fonction des menaces prévisibles.
Conformité réglementaire et suivi des exigences	Restez informés des lois et normes applicables dans votre secteur et veillez à votre conformité. En Belgique, les autorités (CCB) ont publié le référentiel CyberFundamentals qui détaille les mesures minimales attendues selon NIS2. Assurez-vous de répondre à ces mesures ou à celles d'une norme équivalente (ISO 27001:2022) pour prouver que vous gérez bien les risques. Note : Infrabel pourra vous demander des preuves de cette conformité (par exemple, un rapport d'audit externe ou un certificat) lors de la qualification ou du suivi de votre contrat.
Processus de gestion documentaire et amélioration continue	Mettez en place un ISMS à votre échelle, même simplifié, incluant la tenue à jour de la documentation (politiques, procédures, inventaires d'actifs, plans d'actions) et des audits internes périodiques. L'objectif est d'inscrire la sécurité dans un cycle d'amélioration continue Plan-Do-Check-Act conformément à ISO 27001. Exemple : un fournisseur d'Infrabel tient un registre des incidents de sécurité survenus dans son périmètre et réalise chaque année un audit

	interne de son dispositif, afin d'identifier des axes d'amélioration, démontrant ainsi sa maturité en gouvernance.

Souveraineté numérique, technologique et stratégique

Pourquoi ?

Infrabel, en tant qu'infrastructure ferroviaire critique, doit garantir sa souveraineté face aux risques digitaux et liés à sa Supply Chain. Cela signifie garder le contrôle sur ses données sensibles, sur les technologies et les composants clés utilisés, et sur ses décisions stratégiques, sans dépendances excessives ni ingérences extérieures.

C'est un pilier de la cyber-résilience nationale : une perte de maîtrise sur des données ou systèmes critiques exposerait Infrabel à des risques majeurs, et l'entreprise pourrait devenir un levier géopolitique pour des acteurs malveillants. Les récents cadres réglementaires renforcent d'ailleurs cette exigence : la directive NIS2 impose aux opérateurs essentiels une gestion rigoureuse des risques, y compris ceux de la chaîne d'approvisionnement et de la gouvernance de la sécurité; le règlement CER vise la résilience des entités critiques et oblige à anticiper les défaillances de fournisseurs pour assurer la continuité des services.

De même, le Cyber Resilience Act (CRA) (règlement UE 2024/2847) introduit dès 2026 des exigences de cybersécurité pour les produits numériques (sécurité par conception, correctifs rapides, divulgation des failles) afin d'améliorer la transparence technologique – par exemple, aucune vulnérabilité connue ne devra subsister lors de la mise sur le marché d'un produit.

Ces obligations rejoignent l'esprit des normes sectorielles : la série IEC 62443 sur la sécurité industrielle fixe des principes techniques et organisationnels repris implicitement dans NIS2, le CRA ou la directive RED, et la future norme ferroviaire IEC 63452 (attendue en 2026) viendra adapter ces principes au rail en clarifiant les responsabilités de chaque acteur (exploitant, intégrateur, fournisseur, etc.), en cohérence avec NIS2 et le CRA. Concrètement, la souveraineté implique pour les fournisseurs d'Infrabel : localiser et protéger les données sensibles sous juridiction de confiance, maîtriser les composants technologiques critiques (logiciels, matériels) tout au long de leur cycle de vie, et anticiper les risques géopolitiques liés à d'éventuelles dépendances hors UE.

Cette approche réduit significativement les risques systémiques : par exemple, NIS2 prévoit que les opérateurs puissent devoir cesser un contrat avec un fournisseur présentant un risque cyber trop élevé.

Infrabel attend donc de ses partenaires une démarche proactive en la matière. L'enjeu s'inscrit dans une responsabilité partagée : chaque maillon de la Supply Chain doit collaborer étroitement, faire preuve de transparence et adopter des standards communs (tels que IEC 62443) pour renforcer la résilience globale.

En résumé, la souveraineté des données, des technologies et des décisions, est désormais indissociable de la cyber-résilience d'Infrabel et de ses fournisseurs.

Mesures attendues

Mesure attendues	Description
Politique et principes de souverenaité	En appliquant ces principes de souveraineté, vous contribuez à pérenniser la sécurité et la résilience d'Infrabel tout en renforçant votre propre position sur un marché de plus en plus exigeant. La souveraineté est un pré-requis opérationnel pour tout fournisseur d'une infrastructure essentielle comme Infrabel. Pour ce faire, Infrabel compte sur chacun de ses partenaires pour innover et s'organiser en conséquence, de la gouvernance aux choix techniques, de manière à ce que la chaîne de valeur ferroviaire demeure sous contrôle, résistante aux chocs externes et conforme aux intérêts stratégiques nationaux et européens.

Contrôles d'accès et protection des systèmes critiques

Pourquoi ?

La gestion des accès aux systèmes et aux données sensibles est l'un des domaines les plus cruciaux (et souvent le premier visé par NIS2, ISO 27001 et NIST CSF). Si un attaquant compromet vos identifiants ou pénètre un réseau critique via un fournisseur, il peut causer de graves dommages.

Infrabel attend donc de ses fournisseurs qu'ils sécurisent rigoureusement l'accès à leurs systèmes, d'autant plus si ceux-ci sont interconnectés à l'infrastructure d'Infrabel.

La directive NIS2 souligne l'importance de « la protection des systèmes critiques et la surveillance des accès » comme mesure prioritaire.

Mesures attendues

Mesure attendues	Description
Contrôle des identités et authentification forte	Assurez-vous que seuls les utilisateurs autorisés accèdent aux ressources, et uniquement aux informations nécessaires à leurs tâches (principe du moindre privilège). Mettez en place une authentification multifacteur (MFA) pour toutes les connexions sensibles, en particulier pour les accès distants et les comptes à privilèges. NIS2 et les bonnes pratiques imposent désormais l'usage généralisé du MFA pour réduire le risque d'usurpation d'identifiants. Exemple : un fournisseur fournissant du support à distance sur des systèmes Infrabel a déployé une solution MFA de dernière génération pour que chaque technicien s'authentifie sur le VPN sécurisé. De plus, des comptes uniques et nominatifs sont créés pour chaque intervenant (pas de compte générique partagé), afin d'assurer une traçabilité.

Gestion des accès à privilèges (PAM)	Identifiez vos comptes administrateurs ou ayant des droits élevés (sur vos systèmes internes ou sur ceux d'Infrabel) et sécurisez-les via un système de gestion des accès à privilèges. Cela inclut : stockage des mots de passe administrateurs dans un coffre-fort électronique sécurisé, activation de logs/alertes sur l'utilisation de ces comptes, et éventuellement approbation à double contrôle pour les actions les plus sensibles. Exemple : un prestataire IT d'Infrabel a mis en place CyberArk (PAM) pour centraliser les comptes admin utilisés chez Infrabel, avec renouvellement fréquent des mots de passe et enregistrement des sessions d'administration. Ce type de mesure répond aux attentes d'Infrabel en matière de contrôle des accès privilégiés.
Segmentation réseau et protection des postes	Si vous hébergez ou traitez des données liées à Infrabel au sein de votre infrastructure, celles-ci doivent résider sur des systèmes et réseaux sécurisés et cloisonnés. Séparez les environnements sensibles (par ex. serveurs connectés aux systèmes Infrabel) du reste de votre réseau d'entreprise par des zones de sécurité dédiées (cf. principes zones & conduits d'IEC 62443). De même, protégez vos postes de travail et serveurs par des outils anti-malware et de gestion des correctifs (voir section suivante). Exemple : un cabinet de conseil, fournisseur d'Infrabel, a mis en place un réseau isolé pour les projets Infrabel, accessible uniquement aux consultants habilités, et avec des postes durcis (antivirus à jour, chiffrement de disque activé, etc.). Ainsi, même en cas d'incident interne, le risque de propagation vers Infrabel est minimisé.
Surveillance des accès et journaux	Maintenez des journaux d'accès et d'activité sur vos systèmes critiques (logs de connexion, actions d'administration, flux réseau sensibles). Ces logs doivent être conservés suffisamment longtemps et révisés régulièrement pour détecter des tentatives suspectes. Des outils de corrélation (SIEM) ou des analyses périodiques peuvent vous aider à repérer des anomalies. C'est une exigence implicite de NIS2 et ISO 27001 (contrôles de journalisation, surveillance continue). Exemple : suite à une recommandation d'Infrabel, un fournisseur a activé la journalisation détaillée sur son serveur SFTP d'échange de fichiers et examine chaque semaine les connexions pour vérifier qu'aucune connexion non attendue ou en dehors des horaires n'ait eu lieu.
Chiffrement des données sensibles	Si vous stockez ou échangez des données d'Infrabel (plans, données d'exploitation, informations personnelles, etc.), celles-ci doivent être chiffrées tant au repos (sur vos serveurs, PC, sauvegardes) qu'en transit

	(communications chiffrées par VPN, TLS, etc.). Par exemple, chiffrez les disques durs contenant des données Infrabel et n'envoyez jamais de données sensibles par e-mail sans chiffrement. Exemple : un fournisseur traitant des données de trafic ferroviaire pour Infrabel utilise un chiffrement AES 256 bits côté serveur de base de données, et ne transfère les données à Infrabel que via des tunnels VPN IPsec homologués, conformément aux politiques d'Infrabel. Objectif : garantir confidentialité et intégrité, comme l'exigent RED et CRA pour les communications et données.

En appliquant ces mesures, vous réduisez significativement les risques d'intrusion et de fuite de données.

NIS2 insiste particulièrement sur la gestion des accès et la protection des systèmes critiques car ce sont souvent par ces chemins que surviennent les incidents majeurs (ex. attaques par mot de passe volé ou mauvaise configuration réseau).

Infrabel audite régulièrement ses propres contrôles d'accès et attend un niveau de vigilance équivalent de la part de ses fournisseurs.

Sécurité par conception et gestion des vulnérabilités

Pourquoi ?

La cyber-résilience implique d'anticiper les attaques en renforçant les systèmes dès leur conception et en corrigeant rapidement les failles.

Deux développements récents rendent cela incontournable : d'une part, le Cyber Resilience Act va exiger des fabricants de produits numériques qu'ils suivent des pratiques de développement sécurisé et de maintenance proactive des correctifs; d'autre part, la directive NIS2 impose aux opérateurs et à leur chaîne de valeur de mettre en place un processus continu de gestion des vulnérabilités (veille, patchs, suivi des correctifs).

Infrabel attend de ses fournisseurs qu'ils démontrent une démarche "Cyber-Resilience-by-Design" et une réactivité exemplaire face aux failles de sécurité.

Mesures attendues

Mesure attendues	Description
Cycle de développement sécurisé (SDLC)	Si vous développez un logiciel, une application ou concevez un système pour Infrabel, intégrez la sécurité à chaque phase de votre cycle de développement. Cela inclut l'analyse de menaces avant la conception (évaluer les scénarios d'attaque potentiels), l'intégration de contrôles de sécurité dans le code et l'architecture (par ex. gestion robuste des erreurs, protections contre l'injection, etc.), des tests de sécurité systématiques

	(analyses de code statique, tests d'intrusion en phase de recette) et la gestion des failles découvertes après livraison. Exemple : un éditeur fournissant un logiciel à Infrabel a mis en œuvre la norme IEC 62443-4-1 (processus de développement sécurisé) : chaque version fait l'objet d'une revue de code orientée sécurité, d'un scan de vulnérabilités automatique, et les développeurs ont été formés aux bonnes pratiques de codage sûr. Ainsi, le produit répond aux critères « Secure-by-Design » du CRA (aucune vulnérabilité connue à la livraison).
Gestion des vulnérabilités et des correctifs	Établissez un processus de veille de sécurité pour être informé rapidement des nouvelles vulnérabilités affectant vos produits, systèmes ou dépendances (ex. abonnements aux alertes CERT, CVE, etc.). Mettez en place une procédure de patch management avec des délais maximum d'application des correctifs : les failles critiques doivent idéalement être corrigées sous quelques jours. Documentez clairement ce processus et, si une vulnérabilité majeure touche un composant utilisé par Infrabel, informez-en sans délai les interlocuteurs Infrabel concernés. Exemple : un fournisseur responsable de la maintenance d'un système SCADA industriel pour Infrabel a défini un calendrier de mises à jour mensuelles (pour les correctifs standard) et un processus d'hotfix sous 48 heures pour toute faille critique. Lors de la divulgation de Log4Shell fin 2021, ce fournisseur a identifié sous 24 h les applications vulnérables dans son périmètre Infrabel et déployé les patchs correctifs en moins de 4 jours, conformément aux attentes d'Infrabel.
Communication et transparence (Coordinated Disclosure)	Le CRA introduit l'obligation pour les fournisseurs de produits numériques de mettre en place un mécanisme de divulgation coordonnée des vulnérabilités (CVD). Concrètement, vous devriez fournir un point de contact (e-mail sécurité, portail) où les chercheurs ou clients peuvent vous signaler une faille, et vous engager à leur répondre et à publier des correctifs dans des délais raisonnables. Infrabel valorise les fournisseurs jouant cette transparence. Exemple : sur son site web B2B, un fournisseur de solutions IoT a publié une politique de divulgation de vulnérabilités, s'engageant à accuser réception sous 72 h et à fournir un correctif ou contournement sous 21 jours pour toute faille jugée critique. Ce type d'initiative témoigne d'une culture de sécurité mature et sera apprécié lors de l'évaluation de vos offres.

Maintenance sécuritaire des équipements industriels	Pour les fournisseurs de matériel ou logiciels opérationnels (OT) déployés dans l'infrastructure d'Infrabel, la phase de maintenance en conditions de sécurité (MCS) est tout aussi importante que la livraison initiale. Il convient de prévoir des mises à jour de firmware, des patchs de sécurité pour toute la durée de vie du produit, et de documenter ces engagements dans les contrats. Les IEC 62443-3-3 et 62443-2-4 détaillent par exemple les exigences de maintenance sécuritaire pour les systèmes et les fournisseurs de services. Exemple : un constructeur d'automatismes ferroviaires fournissant à Infrabel des postes de signalisation s'est engagé, via une clause contractuelle, à assurer un soutien sécurité pendant 10 ans (fourniture de mises à jour logicielles, monitoring des vulnérabilités sur ses composants, notification à Infrabel en cas de fin de support anticipée). Ainsi, Infrabel peut intégrer ces éléments dans son propre plan de gestion des actifs et s'assurer que le système reste en conformité vis-à-vis des nouvelles menaces (comme exigé par NIS2 pour les systèmes critiques).

En résumé, montrez qu'aucune faille connue ne subsiste sans plan d'action chez vous. Les études montrent que plus de la moitié des PME victimes d'une cyberattaque majeure font faillite dans les six mois. Ne pas être réactif sur les correctifs peut non seulement vous coûter votre réputation auprès d'Infrabel, mais aussi compromettre votre survie économique.

À l'inverse, une démarche proactive de sécurité par conception et de gestion agile des vulnérabilités sera un facteur de confiance déterminant pour Infrabel.

Surveillance, détection et alertes précoces

Pourquoi ?

Malgré toutes les mesures de prévention, un incident peut survenir. La capacité à détecter rapidement une anomalie ou une attaque est alors déterminante pour limiter l'impact.

NIS2 et les standards comme ISO 27001 exigent la mise en place de dispositifs de supervision de la sécurité et de détection des incidents. Infrabel, de son côté, opère un CyberSOC 24/7 pour surveiller ses actifs critiques.

Elle attend de ses fournisseurs, en particulier ceux connectés à ses systèmes, un niveau de vigilance adéquat : si un incident touche un de vos systèmes liés à Infrabel, vous devez pouvoir le détecter et en alerter Infrabel sans délai.

Mesures attendues

Mesure attendues	Description
Supervision continue (CyberSOC)	En fonction de la taille de votre organisation et de la criticité de vos services, mettez en place une équipe ou un service de supervision sécurité. Cela peut aller d'un simple système d'alertes automatiques sur événements inhabituels, jusqu'à un véritable CyberSOC interne ou externalisé qui analyse en temps réel les logs et comportements. Exemple : une entreprise moyenne, fournisseur d'Infrabel, a souscrit à une offre de CyberSOC externalisé qui surveille ses serveurs et firewall 24/7. Une nuit, une activité anormale a été détectée (scan réseau suspect), le CyberSOC a immédiatement alerté le référent sécurité du fournisseur, permettant de bloquer l'adresse IP malveillante dans la foulée. Ce type de service proactif rejoint l'approche d'Infrabel, qui a également recours à un CyberSOC externe pour renforcer sa détection.
Systèmes de détection des intrusions (IDS/IPS)	Sur vos réseaux et systèmes critiques, déployez des outils de détection automatisée : pare-feu de nouvelle génération avec inspection profonde, sondes IDS réseau, agents EDR (Endpoint Detection & Response) sur les postes/serveurs, etc. Ces outils remontent des alertes en cas d'activité indicative d'une attaque (malware connu, comportement anormal, tentative d'accès interdit). Ils doivent être configurés de manière à couvrir les points d'entrée possibles vers les données/systèmes liés à Infrabel. Exemple : un hébergeur de données pour Infrabel a installé une sonde IDS sur le segment réseau hébergeant les serveurs du projet, configurée avec les signatures de menaces les plus récentes. Un jour, la sonde a détecté une tentative d'exploiter une vulnérabilité connue sur un serveur web : l'alerte a été corrélée et a déclenché automatiquement le blocage de l'IP source par le firewall (IPS), évitant une possible compromission. Objectif : ne pas dépendre uniquement de la vigilance humaine, mais avoir des "capteurs" actifs en permanence.
Gestion des journaux et corrélation	Assurez-vous que les journaux (logs) issus de vos serveurs, applications, équipements de sécurité, etc., soient rassemblés et analysés de manière cohérente. Un SIEM (Security Information and Event Management) peut agréger ces données et permettre des corrélations (par ex. déceler qu'une même adresse IP a échoué à se connecter 5 fois sur le VPN + scanné un port sur un serveur). Si vous n'avez pas de SIEM, veillez au moins à ce qu'un responsable examine fréquemment les logs essentiels manuellement ou à l'aide d'outils simples.

	Exemple : un fournisseur a configuré l'envoi des journaux de ses appliances (firewall, VPN) vers la plateforme de log d'Infrabel ou vers un SIEM commun. Ainsi, Infrabel pourrait également avoir de la visibilité sur des tentatives d'intrusion visant ce fournisseur et l'anticiper de son côté, c'est une approche collaborative gagnant-gagnant.
Détection des fuites de données (DLP)	Si vous traitez des informations sensibles d'Infrabel, envisagez des solutions pour prévenir et détecter les fuites de données, que ce soit par négligence ou malveillance interne. Des systèmes DLP peuvent surveiller les sorties de données (emails, transferts fichiers) et générer des alertes si, par exemple, un document confidentiel est envoyé en dehors du domaine autorisé. Exemple : une société de conseil manipulant des plans techniques d'Infrabel a mis en place une règle DLP sur sa messagerie : tout email sortant contenant des termes sensibles ou des pièces jointes volumineuses est signalé au RSSI. Un jour, un employé a tenté de s'envoyer sur sa boîte personnelle un document Infrabel (pour travailler chez lui), le système a bloqué l'email et informé l'équipe sécurité, évitant une enfreinte aux règles de confidentialité.

En mettant l'accent sur la détection précoce, vous augmentez fortement vos chances de contenir un incident avant qu'il ne cause des dégâts importants.

Infrabel considère la surveillance continue comme un élément clé de la résilience : « Prévenir, détecter, investiguer et répondre aux cybermenaces 24h/24 » est l'objectif annoncé de son CyberSOC. Elle attend de vous une philosophie similaire, adaptée à votre contexte.

Réponse aux incidents et reprise d'activité

Pourquoi ?

Aucune défense n'est infaillible à 100%. Il faut donc préparer l'organisation à réagir efficacement en cas d'incident (cyberattaque, panne majeure, brèche de données), afin d'en limiter l'impact et d'assurer une reprise rapide.

La capacité de réponse et de reprise, c'est le cœur de la cyber-résilience, est un volet explicitement adressé par NIS2 (plans de gestion de crise, continuité d'activité) et par les normes de système de management (ISO 27001, ISO 22301 pour la continuité, NIST CSF fonction Recover).

Un fournisseur d'Infrabel doit être en mesure non seulement de traiter ses propres incidents, mais aussi de collaborer avec Infrabel en cas d'incident affectant leurs échanges ou l'infrastructure commune.

Mesures attendues

Mesure attendues	Description
Plan de réponse aux incidents (CSIRT)	Élaborez un plan de gestion des incidents de sécurité qui détaille les étapes à suivre en cas d'attaque avérée ou de suspicion sérieuse (procédure CSIRT). Ce plan doit prévoir : les rôles de chacun (qui coordonne, qui enquête, qui communique), les ressources de secours mobilisables, les moyens techniques pour contenir l'incident (isolement de serveurs, blocage de comptes…), ainsi que les contacts à alerter (y compris Infrabel le cas échéant). Entraînez-vous via des exercices ou simulations au moins une fois par an, afin que votre équipe soit familière du processus. Exemple : une société de service, fournisseur d'Infrabel, a formalisé un playbook d'incident : "si ransomware détecté sur un serveur : 1) déclencher le mode dégradé, 2) isoler le serveur du réseau, 3) alerter immédiatement le responsable IT et le RSSI, 4) informer Infrabel si des données ou services partagés sont touchés, 5) analyser l'ampleur, etc.". Ce plan, revu tous les ans, a permis le jour venu de réagir vite et dans le calme lors d'une attaque par cryptovirus, évitant sa propagation.
Notification et communication d'incident	Informez Infrabel sans délai si un incident de sécurité survient et présente un lien avec les activités que vous menez pour Infrabel. Par exemple, si vos systèmes hébergeant des données Infrabel ou connectés à son réseau sont compromis, ou si vous détectez une attaque qui pourrait s'étendre à Infrabel, vous devez le notifier immédiatement. La transparence est cruciale : Infrabel préfère apprendre la nouvelle rapidement de votre part plutôt que via les médias. Par ailleurs, NIS2 impose aux entités essentielles de notifier leur autorité dans les 24 heures suivant la détection d'un incident grave, ce délai ultra-court se répercute donc sur les fournisseurs critiques. Exemple : en 2025, un prestataire d'Infrabel a été victime d'un vol de matériel contenant des données sensibles. Conformément à son contrat et aux bonnes pratiques, il a prévenu immédiatement Infrabel, permettant de déclencher ensemble les mesures (changement des mots de passe compromis, communication conjointe si nécessaire aux personnes affectées, etc.). Rappel : en cas de fuite de données personnelles, le RGPD impose aussi une notification à l'autorité sous 72 h, ne l'oubliez pas.
Plan de continuité d'activité (PCA)	Développez et testez un plan de continuité pour vos services critiques, incluant les scénarios d'incident cyber. L'objectif est d'assurer un niveau

	de service minimal même en situation de crise et de retrouver un fonctionnement normal dans les meilleurs délais (objectif de temps de rétablissement, RTO). Identifiez vos processus essentiels liés à Infrabel et prévoyez des solutions de secours (systèmes de rechange, sauvegardes offline, capacités manuelles temporaires, etc.). NIS2 exige explicitement l'existence de plans de continuité et reprise après sinistre pour les opérateurs et leurs prestataires. Exemple : un fournisseur important fournissant une plateforme en ligne utilisée par Infrabel a établi un PCA : en cas de cyberattaque majeure rendant la plateforme indisponible, un site de secours hébergé sur un autre cloud peut être activé en 4 heures, avec restauration des données depuis la dernière sauvegarde (J-1). Des exercices de bascule sont menés tous les 6 mois. Ainsi, Infrabel sait que même en cas d'incident grave, le service sera remis en route rapidement, ce qui est un facteur de résilience et de conformité.
Rétablissement et leçons apprises	Après tout incident, même mineur, procédez à une analyse post-incident afin d'identifier la cause première, de corriger les faiblesses exploitées et d'améliorer vos processus. Partagez avec Infrabel les conclusions si cela est pertinent (par exemple, si l'incident révèle un risque systémique ou une attaque qui pourrait viser d'autres partenaires). Cette démarche d'amélioration continue fait partie des attentes d'Infrabel et contribue à renforcer le partenariat. Exemple : suite à un incident de phishing ayant piégé un de ses employés, un fournisseur a découvert un manque de filtrage sur sa messagerie. Il a alors implémenté un filtrage anti-spam renforcé et mené une campagne de re-sensibilisation interne, tout en informant Infrabel du vecteur d'attaque utilisé afin que tout le monde se méfie de ce type d'e-mail.

En somme, soyez prêts à « encaisser le choc » et à rebondir. Une réaction rapide et coordonnée réduit drastiquement les dommages financiers, opérationnels et juridiques.

À l'inverse, une réponse chaotique ou tardive peut transformer un incident modéré en véritable crise. Infrabel investit fortement dans sa propre capacité de réponse (équipe CSIRT, procédures de crise, etc.), votre préparation vient compléter ce dispositif global de résilience de la chaîne de valeur.

Sécurité de la chaîne d'approvisionnement et des tiers

Pourquoi ?

« On n'est jamais plus fort que son maillon le plus faible ». Les attaquants l'ont bien compris et cherchent souvent à compromettre une cible en passant par ses fournisseurs ou sous-traitants (attaques de supply chain).

La directive NIS2 consacre ainsi explicitement la sécurité des chaînes d'approvisionnement : les organisations doivent gérer les risques posés par leurs prestataires et imposer des mesures contractuelles aux fournisseurs critiques.

Pour Infrabel, dont la mission est critique, il est impératif que tous les fournisseurs appliquent des standards de sécurité élevés, et que la sécurité soit prise en compte dès la phase d'appel d'offres et tout au long du contrat.

Mesures attendues

Mesure attendues	Description
Intégration de la sécurité dans les contrats	Attendez-vous à ce qu'Infrabel inclue dans ses cahiers des charges et contrats des exigences précises de sécurité de l'information. Par exemple : clauses de conformité NIS2/CER/CRA, clauses techniques (chiffrement, patch management), exigences de certification (ISO 27001 ou autre) ou droits d'audit. Vous devez accepter et respecter ces clauses. Si vous-même faites appel à des sous-traitants pour exécuter une partie du contrat, vous devez répercuter ces exigences vers eux. Exemple : Infrabel prévoit des clauses types de sécurité à inclure dans tout contrat fournisseur. Ces clauses couvrent la gestion des accès, la protection des données, la notification des incidents, etc., et sont modulées selon que le fournisseur accède (ou non) à des données Infrabel, à ses réseaux, ou fournit un service cloud (plus l'exposition est grande, plus les exigences sont élevées). Assurez-vous d'en prendre connaissance dès l'appel d'offres pour pouvoir y répondre correctement.
Évaluation sécurité des fournisseurs en amont	Si vous-même sous-traitez ou utilisez des produits tiers dans le cadre du projet Infrabel, il faut évaluer leurs pratiques de sécurité. Choisissez de préférence des partenaires certifiés (ISO 27001, label CyFun) ou vérifiez via des questionnaires/entretiens qu'ils respectent un niveau de sécurité adéquat. ISO 27001:2022 a introduit des contrôles spécifiques (A.5.19, A.5.22) sur la gestion de la sécurité des relations fournisseurs, incluant la définition d'exigences sécurité dans les contrats, le contrôle de leur mise en œuvre et la revue périodique des fournisseurs. Alignez-vous sur ces bonnes pratiques.

	Exemple : une entreprise fournisseur d'Infrabel (pour un développement logiciel) a dû engager un autre prestataire pour une partie du code. Elle a d'abord fait remplir à ce sous-traitant un questionnaire de sécurité et a intégré les résultats dans son analyse de risques du projet. Ainsi, Infrabel a été rassurée de voir que la société maîtrisait sa propre supply chain et ne choisissait pas ses partenaires sans prendre les précautions qui s'imposent.
Suivi et audits des fournisseurs critiques	Tout au long d'un contrat, il convient de surveiller le respect des exigences par les fournisseurs et partenaires. Infrabel se réserve le droit d'auditer ses fournisseurs sur les aspects sécurité, vous devez donc être prêts à fournir des informations ou à accueillir un audit le cas échéant. De votre côté, n'hésitez pas à demander périodiquement des comptes-rendus ou attestations à vos propres sous-traitants critiques. Exemple : le département sécurité d'Infrabel organise des contrôles annuels chez certains prestataires sensibles : vérification des mesures en place, tests de pénétration conjointe, etc. Un fournisseur anticipatif pourrait lui-même réaliser un audit externe de son dispositif et le transmettre spontanément à Infrabel en gage de sérieux. Point d'attention : NIS2 prévoit que les opérateurs essentiels (comme Infrabel) pourront être contraints par leur autorité à suspendre ou mettre fin à un contrat avec un fournisseur qui présenterait un risque cyber élevé. Nous espérons ne jamais en arriver là, et votre coopération proactive évitera ces situations extrêmes.
Restitution des données et fin de contrat	Lorsque votre mission ou contrat avec Infrabel se termine, assurez-vous de retourner ou détruire de façon sécurisée toutes les informations d'Infrabel en votre possession, conformément aux clauses contractuelles. Cela fait partie intégrante du cycle de vie sécurisé du fournisseur. Exemple : un fournisseur logistique a, en fin de contrat, restitué à Infrabel l'ensemble des jeux de données d'exploitation mis à sa disposition et fourni un certificat d'effacement prouvant que toutes les copies de ces données ont été supprimées de ses serveurs et sauvegardes. Ce niveau de rigueur clôt le partenariat sur une note positive et assure qu'aucune "bombe à retardement" ne subsiste après votre départ.

En synthèse, la sécurité est l'affaire de toute la chaîne. Infrabel intègre désormais systématiquement des considérations de sécurité dans son processus achat (évaluation des risques avant, pendant et après le contrat). Les fournisseurs sont tenus d'y collaborer activement. En démontrant une maturité dans la gestion de votre propre écosystème de sous-traitants, vous vous positionnez comme un partenaire de confiance.

À l'inverse, toute faiblesse notoire chez un fournisseur pourrait remettre en cause la relation commerciale (par obligation légale pour Infrabel).

Sensibilisation du personnel et culture de sécurité

Pourquoi ?

L'aspect humain reste souvent le maillon faible en cybersécurité. Une politique et des technologies ne suffisent pas si les employés ou partenaires qui les utilisent ne sont pas sensibilisés aux risques. De nombreuses attaques (phishing, ingénierie sociale) ciblent directement les individus.

La directive NIS2 insiste sur la formation du personnel à la sécurité, et l'ISO 27001 consacre plusieurs contrôles à la sensibilisation et aux compétences. Infrabel mène régulièrement des campagnes internes sur ces sujets (e-learning, tests de phishing, communications).

Il est attendu que les fournisseurs en fassent de même avec leurs propres équipes, surtout celles en lien avec des informations ou systèmes d'Infrabel.

Mesures attendues

Mesure attendues	Description
Formations initiales et continues	Veillez à ce que chaque collaborateur de votre entreprise, en particulier ceux affectés à des projets Infrabel, reçoive une formation de base en cybersécurité. Celle-ci doit couvrir les bonnes pratiques de protection et la sensibilisation aux menaces courantes (phishing, malware, fraude). Renforcez ces notions par des sessions régulières (par ex. annuelles) ou de courts modules e-learning. Exemple : un prestataire de maintenance a inscrit tous ses techniciens à une formation en ligne « Cybersecurity », qui aborde les bonnes pratiques, la gestion des risques, la gestion des fournisseurs et le « Security by Design ». Ainsi, ces techniciens connaissent l'essentiel et intègrent naturellement la sécurité dans leurs interventions.
Sensibilisation ciblée (phishing, fraude)	Mettez en place des exercices de simulation (ex. envoi de faux e-mails de phishing pour tester la réaction) et partagez régulièrement des alertes ou anecdotes sur les cybermenaces qui pourraient vous viser. Encouragez une culture où l'on ose signaler un incident ou un e-mail suspect sans crainte de blâme, mieux vaut un faux positif que laisser passer un malware. Exemple : une entreprise fournisseur a mis en place un bouton "Signaler un e-mail suspect" dans Outlook pour ses employés, relié à son équipe sécurité, reprenant une initiative d'Infrabel. Résultat : le taux de clic sur des mails piégés lors des exercices de phishing internes a chuté de 15% à 3% en un an, signe d'une vigilance accrue du personnel.

Communication interne sur la sécurité	Relayer les messages clés de la sécurité de l'information via vos canaux internes (réunions, affiches, newsletters). Insistez sur le fait que la sécurité est l'affaire de tous, et pas seulement du service IT. Valorisez les bons comportements et les personnes proactives (par ex. un employé ayant évité une escroquerie doit être félicité publiquement, cela incite les autres à être attentifs). Exemple : lors du Mois Européen de la Cybersécurité en octobre, de nombreux employeurs organisent des sensibilisations ludiques (quiz, challenges). Un fournisseur a invité l'équipe I-ICT.14 d'Infrabel à présenter aux employés les dernières menaces dans le secteur ferroviaire et les bons réflexes à adopter. Cette session interactive a rencontré un franc succès et a renforcé la relation de confiance entre Infrabel et le fournisseur, tout en élevant le niveau de conscience de chacun.
Communication interne sur la sécurité	En développant une véritable culture de la cybersécurité au sein de votre organisation, vous réduisez la probabilité d'erreurs humaines coûteuses et vous vous conformez aux attentes réglementaires (par ex. NIS2 exige que "les collaborateurs aient une bonne connaissance de la sécurité de l'information").

Infrabel attache une grande importance à cet aspect humain de la sécurité. Vos efforts dans ce domaine seront donc particulièrement appréciés.

Nous invitons tous nos fournisseurs à prendre contact avec notre équipe afin de participer à une session d'information ou de suivre l'une de nos formations dédiées à la cybersécurité. Ces rencontres sont l'occasion d'approfondir les exigences d'Infrabel, d'échanger sur les bonnes pratiques et de renforcer ensemble la sécurité de l'écosystème ferroviaire.

Clauses contractuelles et exigences de gouvernance

Infrabel utilisera son pouvoir de marché et ses obligations légales pour imposer des clauses de cybersécurité strictes dans tous ses nouveaux contrats. Les cinq clauses indispensables pour un fournisseur sont :

1. **Clause d'audit :** Infrabel se réserve le droit de réaliser des audits de sécurité annuels ou des tests d'intrusion sur les solutions fournies.
2. **Transparence de la sous-traitance :** Le fournisseur doit déclarer ses propres sous-traitants et s'assurer qu'ils respectent les mêmes niveaux de sécurité.
3. **Maintien en condition de sécurité (MCS) :** Le fournisseur s'engage à maintenir les correctifs de sécurité pendant toute la durée de vie contractuelle du produit, avec des SLA de correction stricts (ex: 48h pour une faille critique).
4. **Assurance Cyber :** Preuve que le fournisseur est couvert par une police d'assurance cyber adéquate pour faire face aux conséquences financières d'une faille.

5. **Gestion de fin de vie :** Procédures de destruction sécurisée des données et de récupération des configurations en cas de résiliation.

Conclusion : Vers une collaboration résiliente et conforme

En mettant en œuvre les exigences concrètes détaillées ci-dessus, de la gouvernance aux techniques de protection, en passant par la détection, la réaction et la gestion de vos propres sous-traitants, vous renforcez non seulement la sécurité d'Infrabel mais aussi la vôtre. Les cadres réglementaires comme NIS2 ou le CRA visent à élever le niveau de cybersécurité de tout l'écosystème : Infrabel et ses fournisseurs.

En pratique, nous vous encourageons à formaliser votre conformité à ces exigences. Obtenir une certification ISO/IEC 27001 ou une attestation de conformité au schéma CyberFundamentals du CCB (selon votre catégorie) est une démarche fortement valorisée, apportant une présomption de conformité aux yeux des autorités NIS2 et de vos clients essentiels. De même, participer à des audits de sécurité mutuels ou des échanges de bonnes pratiques avec Infrabel renforcera la confiance et l'efficacité de notre partenariat.

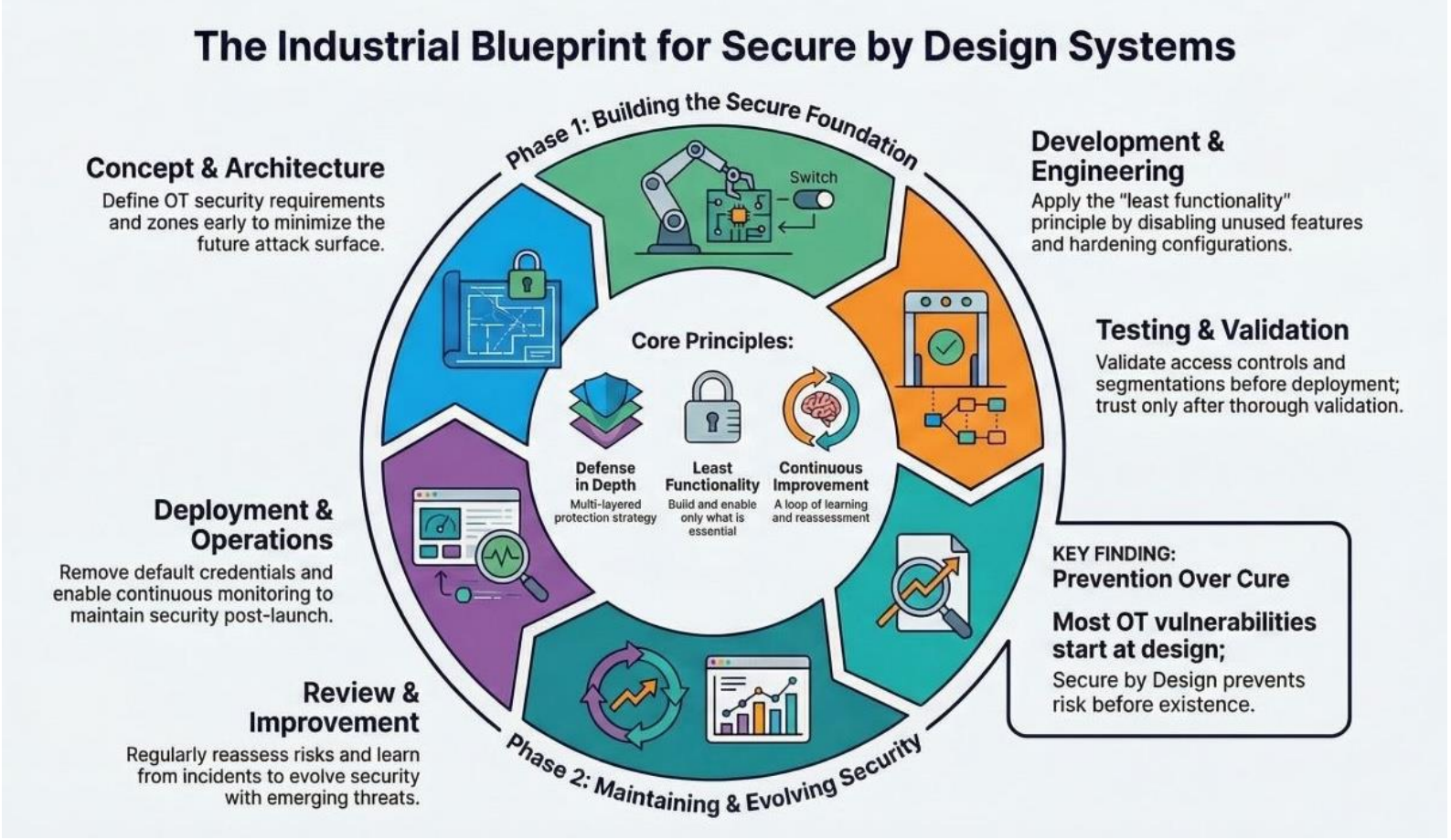
La réglementation cyber va continuer d'évoluer (mise en œuvre du CRA, finalisation d'IEC 63452 niveau ferroviaire, etc.). La clé est d'adopter dès maintenant une posture proactive. En investissant dans la cyber-résilience, vous réduisez vos risques de sanctions, de pertes financières ou d'exclusion de marchés, et vous vous positionnez comme partenaire de confiance sur le long terme. Infrabel est disposée à vous accompagner dans cette montée en maturité, car notre résilience est un effort collectif.

En conclusion, retenez que la cyber-résilience fournisseur s'articule autour de trois principes : anticiper (les risques via la gouvernance et la conception sécurisée), surveiller/réagir (détection continue et réponse efficace), et s'adapter/améliorer (apprentissage et évolution constante). C'est à ce prix que nous pourrons, ensemble, assurer la sécurité et la pérennité des activités ferroviaires face aux menaces numériques croissantes.

Contacts utiles

Canal	Description
ciso@infrabel.be	Pour toute question sur les exigences de sécurité d'Infrabel.
csirt@infrabel.be	En cas d'urgence (suspicion d'attaque), le point de contact d'Infrabel est accessible 24/7.

Nous vous remercions de votre collaboration et de votre engagement à nos côtés pour un avenir digital plus sûr.



POUR DES SYSTEMES INDUSTRIELS « SECURE-BY-DESIGN »

Ce modèle opérationnel de référence préconisé par Infrabel pour les fournisseurs de solutions industrielles repose sur le principe fondamental de « Security-by-Design ».

Ce blueprint, divisé en deux phases majeures, vise à prévenir l'existence même des risques plutôt que de tenter de les guérir a posteriori. L'analyse des vulnérabilités montre que la majorité des failles dans les technologies opérationnelles (OT) prennent racine lors de la phase de conception initiale.

PHASE 1 : Construction d'une fondation sécurisée

La première phase du cycle de vie d'un système industriel sécurisé se concentre sur l'établissement de bases techniques et organisationnelles saines. Elle commence par la définition rigoureuse de l'architecture et des concepts de sécurité.

Le domaine **« Concept & Architecture »** exige que les exigences de sécurité OT et le zonage soient définis dès les premières ébauches du projet afin de minimiser la surface d'attaque future. En s'appuyant sur la norme IEC 62443-3-2, le fournisseur doit segmenter sa solution en zones logiques basées sur le risque et la criticité, chaque zone étant reliée par des « conduits » contrôlés et sécurisés. Cette approche garantit qu'une compromission dans une zone moins critique IT ne puisse pas se propager vers les « joyaux de la couronne » que sont les systèmes critiques opérationnels.

Le domaine **« Développement & Ingénierie »** met en œuvre le principe de la « moindre fonctionnalité » (Least Functionality). Il s'agit par exemple de désactiver systématiquement toutes les fonctions, ports et services inutilisés dans les configurations par défaut des équipements. De plus, le durcissement (hardening) des configurations doit être documenté pour permettre à l'entité essentielle de vérifier l'intégrité du système lors de la réception.

PHASE 2 : Maintenance et évolution de la sécurité

Une fois les fondations posées, la sécurité doit être maintenue et adaptée tout au long de la phase opérationnelle pour faire face à l'évolution constante des menaces.

Le domaine **« Tests & Validation »** constitue le filtre final avant le déploiement. Il impose la validation rigoureuse des contrôles d'accès et des segmentations réseau. Le fournisseur doit adopter une posture de type « Zero Trust », où aucun composant n'est considéré comme sûr sans une validation approfondie des protocoles et des identités. Les tests d'acceptation en usine (FAT) et sur site (SAT) doivent inclure des scénarios de cyber-résilience.

Le domaine **« Déploiement & Opérations »** traite de la transition vers la production réelle. Une mesure impérative est le retrait ou la modification immédiate de tous les identifiants et mots de passe par défaut fournis par le constructeur. Parallèlement, le fournisseur doit activer des capacités de surveillance continue pour maintenir la posture de sécurité post-production. Par exemple, cela inclut l'intégration de sondes IDS industrielles capables de détecter des changements de logique non autorisés dans les systèmes OT.

Le domaine **« Révision & Amélioration »** ferme la boucle par un apprentissage continu. Le fournisseur doit régulièrement réévaluer les risques et tirer les leçons des incidents passés pour faire évoluer ses solutions face aux menaces émergentes. Cette approche itérative est conforme aux exigences de l'IEC 62443-2-1 et de la loi NIS2 sur l'amélioration continue des mesures de gestion des risques.

Implémentation de la norme IEC 62443 pour les fournisseurs d'Infrabel

La série IEC 62443, qu'Infrabel utilise comme norme de référence dans ses cahiers des charges, fournit le cadre technique nécessaire pour répondre aux exigences de la loi NIS2 dans le domaine industriel.

Chaque type de fournisseur doit identifier les parties de la norme qui s'appliquent à son rôle spécifique.

Les fabricants de systèmes de contrôle, de composants réseau et d'applications logicielles industrielles sont les garants de la sécurité intrinsèque des produits (Product Suppliers - 4-1 & 4-2)

Ils doivent démontrer un cycle de vie de développement sécurisé conforme à l'IEC 62443-4-1. Cela inclut le threat modeling dès la phase de design et la gestion rigoureuse des correctifs. Au niveau technique (IEC 62443-4-2), les composants doivent atteindre au minimum le niveau SL 2 pour une entité essentielle, garantissant une résistance aux attaques intentionnelles simples.

Pour les intégrateurs et prestataires (Service Providers - 2-4 & 3-3)

Le programme de sécurité des prestataires (IEC 62443-2-4) exige des politiques strictes pour la maintenance à distance. L'intégrateur est responsable de s'assurer que l'architecture globale respecte les exigences système (IEC 62443-3-3), notamment le contrôle d'utilisation et le flux restreint de données.

Convergence avec le Cyber Resilience Act (CRA)

Il est important de noter que le paysage réglementaire belge s'aligne de plus en plus sur les exigences futures du Cyber Resilience Act (CRA) européen, publié le 20 novembre 2024. Le CRA impose des exigences horizontales de cybersécurité pour tous les produits comportant des éléments numériques.

L'IEC 62443-4-2 est pressentie pour devenir une norme harmonisée sous le CRA. Un fournisseur industriel certifié IEC 62443 aujourd'hui sera donc naturellement prêt pour les obligations du CRA qui deviendront pleinement exécutoires d'ici 2027. Cette convergence facilite grandement la gestion de la conformité : un seul effort de certification permet de répondre à la fois aux exigences contractuelles NIS2 des clients essentiels, comme Infrabel, et aux obligations réglementaires européennes de mise sur le marché.

Exemples de mesures

Domaine	Mesure Industrielle (Exemples)	Référence Normative / Légale
Accès Distant	VPN IPsec/TLS avec MFA obligatoire et passerelle d'accès privilégié (PAM).	IEC 62443-2-4 NIS2 Art. 21
Durcissement	Désactivation des services inutiles (FTP, HTTP non chiffré) et verrouillage des ports USB physiques.	IEC 62443-4-2 CRA Essential Req.
Intégrité	Signature cryptographique du firmware et activation du Secure Boot sur les automates.	IEC 62443-4-2 CRA Annex I
SBOM	Inventaire dynamique des composants logiciels (open-source et propriétaires) mis à jour à chaque release.	IEC 62443-4-1 CRA Article 6
Surveillance	Intégration de sondes IDS OT et exportation des journaux d'audit horodatés vers le CyberSOC d'Infrabel	IEC 62443-3-3 NIS2 Défense
CVD	Publication d'une politique de divulgation coordonnée des vulnérabilités sur le site web du fournisseur.	NIS2 Belgique CRA Part II

Conclusion

En conclusion, la cybersécurité des solutions industrielles pour une entités essentielle belge comme Infrabel n'est plus une simple option technique mais une obligation légale et contractuelle impérative.

En s'appuyant sur le principe de « Secure-by-Design » et en s'alignant sur les standards IEC 62443, les fournisseurs d'Infrabel garantissent non seulement la résilience des infrastructures critiques nationales d'Infrabel mais assurent également leur propre pérennité dans un marché de plus en plus régulé.

L'effort consenti aujourd'hui dans la structuration des processus et le durcissement des produits constitue le meilleur investissement face aux défis cyber de demain.

DES PRODUITS CONFORMES AU CRA

La loi sur la cyber-résilience (CRA) est un règlement horizontal de l'Union européenne, adopté en octobre 2024, qui définit les obligations des fournisseurs proposant des produits comportant des éléments digitaux (PDE) sur le marché européen.

Le CRA définit des exigences de sécurité de base pour tous les produits digitaux mis sur le marché de l'UE. Il s'applique à tous les types de produits, des appareils intelligents et des systèmes embarqués aux outils logiciels purs. Si votre produit se connecte à un réseau, il est fort probable qu'il soit concerné.

Le règlement CRA instaure également un nouveau niveau de responsabilité tout au long de la chaîne d'approvisionnement des produits numériques. Vous êtes tenu de considérer la cybersécurité comme une exigence fondamentale du produit, et non comme une fonctionnalité supplémentaire. Ce règlement intègre la sécurité dès les premières étapes du développement et de l'approvisionnement.

Objectif et contexte législatif

Avant l'entrée en vigueur de la CRA, les règles en matière de cybersécurité variaient d'un pays à l'autre. Cela engendrait une certaine confusion et laissait des lacunes dans l'ensemble du paysage des produits.

Le CRA remplace ce patchwork par un cadre clair applicable à tous les États membres de l'UE.

Pourquoi est-ce important pour les responsables de la sécurité des produits ?

Votre rôle ne se limite pas à cocher des cases : il s'agit de protéger les utilisateurs et de soutenir les objectifs de l'entreprise. Le CRA vous offre une voie claire pour atteindre ces deux objectifs. Une préparation précoce aide votre équipe à rester sécurisée, conforme et compétitive.

Le CRA vu par l'EIM (European Infrastructure Managers)

L'EIM, dont Infrabel est un membre actif, salue la CRA et le changement de paradigme fondamental en matière de sécurité numérique qu'elle entraîne au sein de l'UE : le niveau actuel de cybersécurité des PDE est faible et doit être renforcé afin de réduire les cyberrisques dans tous les secteurs. Le CRA couvre l'ensemble du cycle de vie du produit, depuis la planification, la conception, le développement ou la production, les essais et la maintenance, jusqu'à sa mise hors service.

Bien qu'il s'agisse d'une législation horizontale applicable à de nombreux secteurs, la CRA contient des dispositions spécifiques reconnaissant que certains PDE doivent se conformer à une législation sectorielle (telle que les spécifications techniques d'interopérabilité (STI)) et, par conséquent, peuvent devoir s'écarter de certaines exigences essentielles de la CRA. À cette fin, elle établit des mécanismes clairs permettant de tenir compte de telles situations.

En outre, comme indiqué dans le préambule, la CRA vise à compléter le cadre juridique établi par la directive NIS2 en garantissant que les produits matériels et logiciels utilisés par les gestionnaires d'infrastructures répondent à certaines exigences essentielles en matière de cybersécurité.

Sécuriser vos produits conformément à la loi européenne sur la cyber-résilience (CRA) grâce aux SBOM

Tout PDE mis sur le marché à compter du 11 décembre 2027 devra se conformer aux exigences essentielles de cybersécurité prévues par le CRA, et le fabricant devra assurer un soutien en matière de vulnérabilité pour ce PDE pendant toute sa durée de vie prévue.

Pour les équipes qui développent des appareils connectés, il ne s'agit plus seulement d'innovation. Le CRA instaure la première réglementation unifiée en matière de cybersécurité. Les « Software Bill of Material » (SBOM) sont désormais une obligation, et non plus un simple atout.

Qu'est-ce que la loi européenne sur la cyber-résilience (CRA) ?

Pourquoi les SBOM sont-elles essentielles pour se conformer à la CRA ?

Les SBOM vous permettent de connaître en détail tous les composants logiciels utilisés dans votre produit. Cette visibilité est essentielle pour identifier les vulnérabilités et y répondre rapidement. Les exigences de la CRA en matière de SBOM reposent sur l'idée qu'une visibilité totale est nécessaire pour garantir la sécurité et la conformité.

En vertu de la CRA, les SBOM ne sont pas seulement destinées à un usage interne, elles font partie du dossier technique officiel de votre produit. Si les autorités de surveillance du marché en font la demande, vous devez fournir une SBOM à jour avec des origines logicielles traçables. Le fait de disposer de ce document montre aux régulateurs que vous prenez la transparence et la sécurité au sérieux.

Le rôle des SBOM dans la sécurité des produits

Une SBOM agit comme une nomenclature numérique, vous indiquant ce que contient votre code. Elle inclut les bibliothèques, les paquets et les composants tiers susceptibles de présenter des risques de sécurité. Grâce à ces informations, vous pouvez surveiller les problèmes et agir rapidement lorsque des menaces apparaissent.

Avantages pour les fabricants et les développeurs

Les SBOM offrent à votre équipe un avantage concret, quel que soit le poste occupé. Par exemple :

- Les développeurs peuvent suivre les dépendances et identifier les risques plus tôt
- Les responsables de la sécurité peuvent associer les vulnérabilités connues à des composants réels
- Les responsables de la conformité disposent d'une documentation claire et à jour pour les audits

Qui doit se conformer au CRA ?

Le CRA ne s'applique pas uniquement aux fabricants. Cela inclut les importateurs, les distributeurs et divers acteurs au sein des équipes chargées des produits et de la sécurité.

Chaque acteur de la chaîne d'approvisionnement doit également comprendre comment la conformité au CRA s'articule avec d'autres réglementations de l'UE, telles que la directive NIS2. Vous pouvez être soumis à plusieurs cadres réglementaires en fonction de votre secteur d'activité ou de votre modèle

de déploiement. L'adoption d'une approche harmonisée entre les équipes permettra d'éviter les doublons et les manquements aux obligations.

Fabricants

Vous êtes tenus d'intégrer la cybersécurité dans le produit dès le début. Cela inclut la création et la mise à jour d'une SBOM, la réalisation d'évaluations des risques et la documentation des réponses aux incidents.

Certains produits peuvent nécessiter une évaluation de conformité par un tiers en fonction de leur niveau de criticité.

Importateurs

Vous devez vous assurer que les produits que vous importez dans l'UE respectent les exigences de la CRA. Cela implique notamment de vérifier :

- Que le fabricant a procédé à une évaluation des risques
- Qu'une liste des composants logiciels (SBOM) à jour et la documentation correspondante sont disponibles
- Que le produit porte les marquages de conformité appropriés

Le non-respect de ces vérifications peut entraîner des problèmes juridiques ou des difficultés d'accès au marché.

Distributeurs

Vous êtes tenu de vérifier que chaque produit que vous distribuez respecte les obligations liées à la CRA. Cela implique notamment de vous assurer que les SBOM et les registres de conformité sont en place. Si ce n'est pas le cas, le produit ne peut pas être vendu légalement au sein de l'UE.

Responsable PSIRT

Dans le cadre de la CRA, la gestion des vulnérabilités devient une responsabilité officielle. Vous devrez surveiller les risques, signaler les vulnérabilités graves dans les 24 heures et coordonner l'application des correctifs sur l'ensemble des produits.

Responsable de la conformité

Vous devez assurer le suivi de la conformité tout au long du cycle de vie des produits. Cela implique notamment de conserver les SBOM, d'enregistrer les incidents et de conserver la documentation pendant au moins cinq ans. L'utilisation d'un outil de gestion des SBOM peut vous faire gagner des heures de travail manuel et réduire le stress lié aux audits.

Quels sont les produits concernés par le CRA ?

Tout produit comportant des éléments numériques et vendu dans l'UE est susceptible d'être concerné. Cela inclut les appareils grand public, les systèmes de contrôle industriel, les applications mobiles et les micrologiciels. Les produits appartenant à des secteurs strictement réglementés, tels que l'automobile ou la défense, peuvent être soumis à des règles différentes.

Quel est l'impact de la CRA sur la sécurité du micrologiciel des appareils ?

Dans le cadre de la CRA, le micrologiciel est considéré comme un logiciel. Vous devrez donc assurer le suivi des vulnérabilités, tenir à jour une liste des composants logiciels (SBOM) et garantir la disponibilité des mises à jour pendant toute la durée de la prise en charge.

En quoi la transparence des SBOM facilite-t-elle la gestion des vulnérabilités dans le cadre de la CRA ?

Les SBOM vous indiquent la composition de vos logiciels, y compris les composants tiers et open source. Ainsi, lorsqu'une nouvelle vulnérabilité CVE est signalée, vous savez immédiatement si vous êtes concerné. Cela réduit votre temps de réaction et renforce la gestion des incidents.

Pourquoi la SBOM est-elle importante pour la sécurité des produits ?

Les SBOM rendent les chaînes d'approvisionnement logicielles visibles et gérables. Elles vous aident à détecter les points faibles avant les attaquants et simplifient les rapports de conformité. C'est pourquoi les SBOM sont au cœur des exigences de la CRA en matière de SBOM et de la stratégie moderne de cybersécurité.

Principales exigences du CRA

Le CRA couvre les mesures techniques et organisationnelles visant à protéger les utilisateurs et les systèmes. Comprendre les exigences fondamentales vous aide à savoir par où commencer. Les SBOM ne constituent qu'une partie du tableau.

Le CRA introduit également des niveaux de classification des produits : standard, important et critique. Les produits critiques, tels que les pares-feux ou les systèmes de détection d'intrusion, nécessitent des évaluations de conformité réalisées par des tiers. Connaître la classification de votre produit permet de déterminer quelles obligations s'appliquent et quel doit être le niveau de rigueur de votre approche.

Exigences relatives à la SBOM

Vous devez créer une SBOM pour chaque produit numérique, dans un format tel que SPDX ou CycloneDX. Les recommandations de la loi européenne sur la cyber-résilience concernant la SBOM mettent l'accent sur les dépendances de premier niveau, la lisibilité par machine et la traçabilité entre les différentes versions du produit. Bien que la SBOM ne doive pas nécessairement être rendue publique, elle doit être mise à la disposition des autorités européennes sur simple demande.

Exigences relatives aux vulnérabilités

Vous devrez disposer d'un processus documenté de gestion des vulnérabilités. Cela inclut le suivi des risques liés aux composants via la SBOM, la réponse rapide aux problèmes connus et le signalement des vulnérabilités exploitées via une plateforme centrale. Tout retard ou lacune dans ce processus peut entraîner des sanctions.

Signalement des incidents et documentation des risques

Le CRA exige la preuve que vous avez pris en compte la sécurité dès le premier jour. Cela inclut la documentation des incidents, des risques et des mises à jour de la SBOM liées à chaque version. Vous ne savez pas exactement ce qui relève des exigences du CRA en matière de SBOM? Commencez par examiner la visibilité de vos dépendances et la manière dont vous suivez les vulnérabilités des composants.

Se préparer à la conformité à la CRA grâce aux SBOM

Vous n'avez pas besoin d'attendre les dates limites pour commencer à aligner le développement de vos produits sur les exigences de la CRA. En agissant dès maintenant, vous permettez à votre équipe de bénéficier de lancements plus fluides et de réduire les imprévus. Les SBOM constituent la base de cette démarche.

Le CRA encourage une approche proactive, et non réactive, de la conformité. L'intégration précoce d'outils et de processus SBOM aide votre équipe à détecter les risques avant qu'ils n'affectent les délais de lancement. Cela rend également les audits et la documentation beaucoup moins perturbants par la suite.

Réalisation d'évaluations des risques liés aux produits

Chaque produit doit faire l'objet d'une évaluation des risques de cybersécurité avant son lancement. Vous devez évaluer l'utilisation de logiciels tiers, les surfaces d'attaque et votre capacité à appliquer des correctifs ou à effectuer des mises à jour. Les SBOM vous aident en révélant exactement ce que contient votre base de code et où les risques pourraient se cacher.

Mise en œuvre efficace des SBOM

La création manuelle de SBOM n'est pas évolutive. Utilisez plutôt des outils qui :

- Génèrent des SBOM lors des phases de compilation ou de CI/CD
- Prennent en charge des formats reconnus tels que SPDX ou CycloneDX
- Suivent les changements entre les versions et déclenchent des alertes en cas de nouveaux risques

Intégrer les exigences CRA dans les processus de développement

La sécurité doit faire partie intégrante du développement, et non être ajoutée a posteriori. Vous pouvez mettre en place des vérifications avant la publication, associer les SBOM aux tickets DevSecOps et effectuer des analyses lors des poussées de code. En intégrant cela à votre workflow, vous restez sur la bonne voie et êtes prêt pour les audits.

Application de la loi et impact sur les entreprises

Le CRA prévoit un calendrier d'application précis et des conséquences concrètes en cas de non-conformité. Mais il y a aussi des avantages : les équipes proactives peuvent transformer la conformité en un atout de confiance. Plus vous agissez tôt, plus la transition se fera en douceur.

La CRA comble le fossé entre la sécurité des logiciels et la responsabilité des produits. Une fois l'application de la loi effective, les autorités nationales procéderont à des contrôles et exigeront des preuves de conformité. Être en mesure de démontrer clairement cette conformité vous confère un avantage opérationnel et en termes de réputation.

Calendrier et sanctions

Voici ce que vous devez savoir :

- Le CRA est entré en vigueur le 10 décembre 2024
- La déclaration des vulnérabilités devient obligatoire à compter du 11 septembre 2026
- La conformité totale à la SBOM est requise à compter du 11 décembre 2027
- Sanction maximale : 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel

Vous avez encore du temps, mais certaines obligations sont déjà en vigueur ; attendre jusqu'en 2027 est une décision risquée.

Risques commerciaux et financiers

La non-conformité met en jeu bien plus que la seule responsabilité juridique. Vous pourriez être confronté à :

- Des lancements retardés ou un accès bloqué au marché de l'UE
- Une perte de confiance de la part des clients ou des partenaires
- Des coûts plus élevés dus à des corrections précipitées ou à des retouches de dernière minute

Une préparation précoce vous évite ces écueils et protège vos résultats financiers.

La conformité comme avantage concurrentiel

Le respect des normes CRA montre que vous prenez la sécurité au sérieux. Grâce à un accompagnement tout au long du cycle de vie et à une visibilité totale sur vos processus CRA SBOM dans l'UE, vous renforcez la confiance des régulateurs et des clients.

ÉVALUATION DU CONTEXTE DE LA MENACES

Dans une relation de supply chain entre Infrabel et ses fournisseurs, le contexte de la menace s'inscrit dans une dynamique bidirectionnelle.

D'une part, Infrabel doit anticiper les risques pouvant émerger des fournisseurs, notamment la compromission de composants ou services essentiels susceptibles d'impacter la sécurité de ses infrastructures critiques.

D'autre part, nos fournisseurs eux-mêmes sont exposés à des menaces issues de l'environnement opérationnel d'Infrabel, telles que la propagation de cyberattaques, la pression réglementaire ou encore la divulgation de vulnérabilités pouvant affecter leur réputation et leur activité.

Ce lien réciproque implique que chaque partie doit non seulement protéger ses propres intérêts, mais aussi collaborer étroitement pour identifier et réduire les risques partagés. La transparence, la coordination dans la gestion des vulnérabilités et la mise en œuvre de standards communs comme l'IEC 62443 renforcent la résilience globale de la chaîne d'approvisionnement, tout en assurant la pérennité et la conformité des opérations pour Infrabel et ses fournisseurs.

Crime organisé

Source de risque

Les acteurs du crime organisé regroupent des organisations cybercriminelles structurées telles que des mafias, des gangs ou des officines spécialisées. Ces entités opèrent dans une logique de profit et s'inscrivent dans un écosystème criminel organisé, structuré et en constante évolution.

Cet écosystème repose sur une spécialisation des rôles, incluant notamment :

- Des développeurs de malwares
- Des opérateurs d'attaque
- Des courtiers d'accès initiaux (Initial Access Brokers)
- Des intermédiaires spécialisés dans la revente de données ou d'accès

Ce modèle, souvent qualifié de "Cybercrime-as-a-Service" (CaaS) ou Ransomware-as-a-Service (RaaS), permet une mutualisation des capacités offensives et une industrialisation des attaques.

Les acteurs du crime organisé peuvent également collaborer avec d'autres profils, notamment des officines spécialisées, afin de renforcer leurs capacités techniques ou d'externaliser certaines étapes de l'attaque.

Objectifs visés

Les acteurs du crime organisé poursuivent principalement des objectifs relevant de la catégorie lucratif, telle que définie dans la méthode EBIOS Risk Manager.

Ces objectifs se traduisent concrètement par :

- La recherche de gain financier direct, notamment via des campagnes de rançongiciels visant à bloquer les systèmes et exiger une rançon
- La fraude financière, incluant des mécanismes tels que la fraude au président ou l'escroquerie en ligne

- La monétisation indirecte, par la revente de données sensibles ou d'accès à des systèmes compromis
- L'exploitation de ressources informatiques (botnets, crypto minage)

En complément, certaines opérations relèvent également de la catégorie entrave au fonctionnement, notamment lorsque les cybercriminels provoquent une indisponibilité des systèmes afin d'augmenter la pression sur la victime (ex. chiffrement de données, arrêt de services critiques).

Ainsi, bien que l'objectif final soit financier, les effets opérationnels peuvent impacter fortement la continuité d'activité.

Motivation

Très élevée — les motivations sont exclusivement financières. Les cybercriminels cherchent à maximiser leurs profits en ciblant des organisations critiques ou vulnérables et en exploitant la pression opérationnelle pour obtenir des paiements rapides.

Ressources

Élevées à très élevées — ces acteurs disposent de ressources financières importantes, d'un accès à des outils sophistiqués et d'une organisation structurée. Certains groupes sont capables d'acquérir ou de développer des vulnérabilités 0-day, et d'investir dans des infrastructures d'attaque complexes.

Activité

Très élevée — les cybercriminels mènent des campagnes continues, souvent automatisées, combinant:

- Attaques opportunistes à grande échelle
- Attaques semi-ciblées
- Opérations ciblées sur des organisations à forte valeur.

Modes opératoires

Les acteurs du crime organisé mettent en œuvre des chaînes d'attaque structurées et industrialisées, combinant plusieurs techniques :

- Campagnes de phishing pour l'accès initial
- Exploitation de vulnérabilités sur des systèmes exposés (VPN, serveurs, applications)
- Élévation de privilèges et mouvements latéraux
- Déploiement de rançongiciels avec double extorsion (chiffrement + fuite de données)
- Utilisation de botnets pour des attaques à grande échelle
- Fraudes ciblées (ex. fraude au président)

Ces attaques peuvent être opportunistes ou ciblées, en fonction de la valeur perçue de la cible. La disponibilité de kits d'attaque accessibles en ligne permet également à des acteurs moins expérimentés de mener des attaques efficaces.

Secteurs d'activité ciblés

Les cybercriminels ciblent prioritairement :

- Les infrastructures critiques (transport, énergie) ;
- Les grandes entreprises ;
- Les organisations dépendantes de leur système d'information ;
- Les entités ayant une faible maturité en cybersécurité.

Dans le cas d'Infrabel, le secteur ferroviaire constitue une cible particulièrement attractive en raison de :

- La criticité des services
- La dépendance aux systèmes IT/OT
- La pression opérationnelle favorisant le paiement de rançons

Arsenal d'attaque

Les cybercriminels disposent d'un arsenal varié et en constante évolution :

- rançongiciels (ransomware)
- Kits d'attaque disponibles en ligne
- Infrastructures de commande et contrôle (C2)
- botnets
- outils d'exploitation de vulnérabilités
- Accès initiaux achetés sur des marchés clandestins
- Outils d'exfiltration et de chiffrement de donnée

Faits d'arme

- attaque Colonial Pipeline
- attaque WannaCry

Ces incidents illustrent la capacité des cybercriminels à perturber des infrastructures critiques, génére des impacts économiques majeurs et exploiter des vulnérabilités à grande échelle.

Attaquant étatique

Source de risque

Les attaquants étatiques regroupent les États, leurs agences de renseignement ainsi que les unités cyber militaires. Ces entités disposent d'une organisation structurée, de moyens sophistiqués et conséquents, voire quasi illimités, leur permettant de mener des opérations cyber offensives sur le long terme.

Ces acteurs se caractérisent par leur capacité à conduire des opérations complexes, planifiées et coordonnées, reposant sur des ressources stables et des procédures définies. Ils sont en mesure d'adapter leurs outils et leurs méthodes à la topologie de la cible, et de maintenir un haut niveau de discrétion.

Ils peuvent également recourir à des vecteurs indirects, notamment en compromettant des fournisseurs ou des partenaires, et disposent pour certains de la capacité d'acquérir ou de découvrir des vulnérabilités inconnues (0-day).

Objectifs visés

Les attaquants étatiques poursuivent des objectifs multiples, relevant principalement des catégories suivantes définies dans la méthode EBIOS Risk Manager :

- Espionnage
  - collecte d'informations stratégiques (industrielles, politiques, militaires) ;
  - surveillance durable des systèmes d'information ;
  - acquisition de propriété intellectuelle.
- Prépositionnement stratégique
  - infiltration de systèmes en vue d'actions futures
  - maintien d'un accès persistant à long terme
  - préparation d'opérations de sabotage ou de déstabilisation.
- Influence
  - diffusion d'informations ou désinformation
  - atteinte à l'image d'une organisation ou d'un État
  - manipulation de l'opinion publique
- Entrave au fonctionnement (dans certains cas)
  - sabotage de systèmes critiques
  - perturbation de services essentiels
  - dégradation volontaire des capacités opérationnelles

Ces objectifs s'inscrivent dans une logique de puissance, de souveraineté et d'avantage stratégique, et peuvent évoluer en fonction du contexte géopolitique.

Motivation

Très élevée — motivations stratégiques, politiques, économiques ou militaires. Ces acteurs agissent dans une logique de long terme et d'intérêt national.

Ressources

Très élevées — ressources humaines, techniques et financières quasi illimitées. Capacité à développer ou acquérir des outils avancés, y compris des vulnérabilités 0-day.

Activité

Modérée à élevée : les opérations sont moins fréquentes que celles du crime organisé, mais ciblées, discrètes et menées sur le long terme.

Modes opératoires

Les attaquants étatiques mettent en œuvre des campagnes sophistiquées de type APT (Advanced Persistent Threat), structurées en plusieurs phases :

- compromission initiale ciblée (phishing, supply chain, exploitation de vulnérabilités)
- mise en place de mécanismes de persistance
- élévation de privilèges et mouvements latéraux discrets
- collecte d'informations à long terme

- maintien d'un accès durable
- éventuellement déclenchement d'actions d'impact (sabotage)

Ces attaques sont caractérisées par leur discrétion, leur adaptabilité et leur durée.

Secteurs d'activité ciblés

Les attaquants étatiques ciblent en priorité :

- infrastructures critiques (transport, énergie, santé)
- industries stratégiques
- institutions publiques
- entreprises à forte valeur technologique

Dans le cas d'Infrabel, le secteur ferroviaire constitue une cible stratégique en raison de son rôle dans la continuité nationale et la logistique.

Arsenal d'attaque

- malwares avancés (APT)
- exploits 0-day
- outils de persistance et de furtivité
- infrastructures de commande et contrôle (C2)
- outils d'espionnage et d'exfiltration
- techniques de supply chain

Faits d'arme

- attaque SolarWinds
- attaque Stuxnet

Ces opérations illustrent la capacité des acteurs étatiques à mener des attaques complexes, discrètes et à fort impact stratégique.

Terroriste

Source de risque

Les acteurs terroristes regroupent des cyberterroristes, des cybermilices ou des groupes idéologiques violents utilisant le cyberespace comme un vecteur d'action complémentaire à leurs opérations traditionnelles.

Ces acteurs disposent généralement de moyens techniques limités comparés aux attaquants étatiques ou au crime organisé, mais compensent cette faiblesse par une forte détermination et un ciblage d'infrastructures critiques. Leurs actions sont souvent orientées vers l'impact immédiat et visible.

Leur capacité d'action peut être renforcée par l'utilisation d'outils disponibles en ligne ou par des collaborations opportunistes avec d'autres acteurs (officines spécialisées, cybercriminels).

Objectifs visés

Les acteurs terroristes poursuivent principalement des objectifs relevant de la catégorie entrave au fonctionnement, telle que définie dans la méthode EBIOS Risk Manager. Ces objectifs se traduisent par:

- Entrave au fonctionnement
  - rendre indisponibles des services essentiels (ex. services d'urgence, systèmes critiques)
  - provoquer des arrêts de systèmes industriels ou énergétiques
  - perturber le fonctionnement normal d'une organisation ou d'une infrastructure
  - saturer les systèmes d'information (ex. attaques DDoS)
- Influence
  - amplification médiatique des actions
  - diffusion de messages idéologiques
  - création d'un climat de peur ou d'insécurité

Ces objectifs visent avant tout à produire un impact sociétal fort, en générant une déstabilisation visible et immédiate.

Motivation

Très élevée : motivations idéologiques fortes, souvent associées à une volonté de déstabilisation, de destruction ou de médiatisation.

Ressources

Faibles à modérées : ressources techniques limitées, mais compensées par l'utilisation d'outils accessibles et par une forte détermination.

Activité

Faible à modérée : attaques moins fréquentes mais potentiellement à fort impact, souvent déclenchées dans des contextes spécifiques (tensions, revendications).

Modes opératoires

Les acteurs terroristes mettent en œuvre des modes opératoires relativement simples mais efficaces, orientés vers l'impact immédiat :

- attaques par déni de service (DDoS)
- exploitation de vulnérabilités sur des sites Internet
- défigurations de sites (defacement)
- perturbation de systèmes industriels ou critiques
- combinaison d'actions cyber et médiatiques

Ces attaques sont généralement peu sophistiquées mais ciblées et déterminées, avec une recherche d'effet immédiat.

Secteurs d'activité ciblés

Les acteurs terroristes ciblent prioritairement :

- infrastructures critiques (transport, énergie, santé)
- services publics
- organisations à forte visibilité

Dans le cas d'Infrabel, le secteur ferroviaire constitue une cible stratégique en raison de :

- son rôle dans la continuité des services publics
- son impact sociétal direct
- sa visibilité médiatique

Arsenal d'attaque

- outils de DDoS
- scripts d'exploitation de vulnérabilités
- outils de défacement
- kits d'attaque disponibles en ligne

Faits d'arme

- attaques DDoS contre des services publics et hospitaliers ;
- campagnes de défiguration de sites gouvernementaux ;
- tentatives de perturbation de systèmes industriels.

Ces incidents illustrent la capacité des acteurs terroristes à générer un impact disproportionné par rapport à leurs moyens techniques.

Activiste idéologique

Source de risque

Les activistes idéologiques regroupent des hacktivistes, des collectifs militants ou des communautés mobilisées autour d'une cause politique, sociétale ou environnementale. Ces acteurs utilisent le cyberespace comme un vecteur d'expression et d'action, afin de promouvoir leurs revendications ou dénoncer des organisations.

Contrairement aux acteurs terroristes, leur objectif n'est généralement pas la destruction mais la visibilité et l'influence. Ils peuvent agir de manière spontanée ou coordonnée, souvent via des communautés en ligne ou des réseaux sociaux.

Leur capacité d'action repose sur la mobilisation collective, la viralité des campagnes et l'utilisation d'outils accessibles.

Objectifs visés

Les activistes idéologiques poursuivent principalement des objectifs relevant de la catégorie influence, telle que définie dans la méthode EBIOS Risk Manager. Ces objectifs se traduisent par :

- Influence
  - diffusion d'informations ou de messages militants
  - atteinte à la réputation d'une organisation
  - divulgation de données sensibles pour exposer des pratiques
  - mobilisation de l'opinion publique via les réseaux sociaux
- Entrave au fonctionnement
  - perturbation ponctuelle de services (ex. DDoS)
  - dégradation temporaire de l'image ou des activités
  - blocage symbolique de plateformes ou services

Ces actions visent principalement à créer un impact médiatique et à influencer les perceptions, plutôt qu'à provoquer des dommages durables.

Motivation

Élevée : motivations idéologiques fortes, liées à une cause (politique, environnementale, sociétale). Recherche de visibilité et d'impact médiatique.

Ressources

Faibles à modérées : ressources techniques limitées, mais capacité à mobiliser un grand nombre d'acteurs et à utiliser des outils accessibles.

Activité

Modérée à élevée : activité dépendante de l'actualité et des causes défendues, avec des campagnes pouvant être massives mais ponctuelles.

Modes opératoires

Les activistes idéologiques mettent en œuvre des actions orientées vers la visibilité :

- attaques DDoS visant à rendre indisponibles des services
- défigurations de sites Internet (defacement)
- divulgation de données (leaks)
- campagnes d'influence sur les réseaux sociaux
- mobilisation de communautés en ligne

Ces actions sont souvent revendiquées et accompagnées d'une stratégie de communication visant à amplifier leur impact.

Secteurs d'activité ciblés

Les activistes idéologiques ciblent principalement :

- organisations publiques ou gouvernementales
- entreprises liées à des enjeux sociétaux (énergie, transport, environnement)
- organisations fortement exposées médiatiquement

Dans le cas d'Infrabel, le secteur ferroviaire peut être ciblé en lien avec :

- des enjeux environnementaux

- des décisions politiques ou sociales
- des perturbations visibles du service

Arsenal d'attaque

- outils de DDoS
- scripts de defacement
- plateformes de diffusion (réseaux sociaux)
- outils de divulgation de données
- kits d'attaque accessibles

Faits d'arme

- Anonymous — campagnes de divulgation et DDoS
- Killnet — attaques DDoS coordonnées

Ces actions illustrent la capacité des activistes à mobiliser des communautés et à générer un impact médiatique important.

Officine spécialisée

Source de risque

Les officines spécialisées regroupent des acteurs techniques avancés, parfois qualifiés de « cybermercenaires », disposant d'un haut niveau d'expertise en cybersécurité offensive. Contrairement aux cybercriminels traditionnels, ces acteurs ne ciblent pas nécessairement directement leurs victimes finales, mais interviennent en tant que prestataires ou fournisseurs de capacités offensives.

Ils conçoivent, développent et mettent à disposition des outils d'attaque, des services ou des infrastructures utilisés par d'autres acteurs, tels que des cybercriminels ou des acteurs étatiques. Leur activité s'inscrit dans un modèle économique structuré, contribuant à l'industrialisation des cyberattaques.

Ces acteurs sont souvent à l'origine de la création de kits d'attaque, de malwares ou de services commercialisés sur des marchés clandestins, facilitant ainsi l'accès à des capacités offensives pour des profils moins expérimentés.

Objectifs visés

Les officines spécialisées poursuivent principalement des objectifs relevant de la catégorie lucratif, telle que définie dans la méthode EBIOS Risk Manager.

Ces objectifs se traduisent par :

- Lucratif
  - développement et vente d'outils offensifs (malwares, exploits, kits d'attaque)
  - fourniture de services de piratage à la demande
  - monétisation de capacités techniques (infrastructures, accès, outils)
  - vente de vulnérabilités, y compris potentiellement des vulnérabilités inconnues (0-day)
- Prépositionnement stratégique
  - fourniture d'accès persistants à des systèmes compromis pour des tiers

- participation indirecte à des opérations de long terme menées par d'autres acteurs

Ces objectifs traduisent une logique de prestation technique et de valorisation des compétences offensives, plutôt qu'un ciblage direct des victimes finales.

Motivation

Élevée : motivation principalement financière, basée sur la monétisation de compétences techniques avancées et de services spécialisés.

Ressources

Élevées : forte expertise technique, capacité de développement d'outils sophistiqués, accès à des ressources techniques avancées.

Activité

Modérée à élevée : activité dépendante de la demande, avec une implication indirecte mais structurante dans de nombreuses opérations cyber.

Modes opératoires

Les officines spécialisées interviennent principalement en support ou en amont des attaques, à travers:

- développement de malwares et d'outils d'exploitation
- création et distribution de kits d'attaque
- vente d'accès initiaux à des systèmes compromis
- fourniture d'infrastructures techniques (serveurs, C2, botnets)
- prestations de piratage à la demande

Leur rôle est central dans l'industrialisation des cyberattaques, en facilitant l'accès à des capacités offensives pour d'autres acteurs.

Secteurs d'activité ciblés

Les officines spécialisées ne ciblent pas directement des secteurs spécifiques, mais leurs outils peuvent être utilisés contre :

- infrastructures critiques
- grandes entreprises
- institutions publiques

Dans le contexte d'Infrabel, ces acteurs représentent une menace indirecte, en augmentant le niveau de sophistication des attaques subies.

Arsenal d'attaque

- malwares personnalisés
- exploits (incluant 0-day)
- kits d'attaque
- infrastructures de commande et contrôle (C2)

- outils de persistance et d'évasion
- plateformes de services cybercriminels

Faits d'arme

Les officines spécialisées étant des acteurs de support, leurs actions sont rarement visibles directement. Leur contribution est toutefois observée dans :

- la diffusion de kits d'attaque largement utilisés
- la mise à disposition d'outils utilisés dans des campagnes majeures de ransomware
- le développement d'exploits réutilisés par différents groupes d'attaquants

Ces éléments illustrent leur rôle clé dans la structuration de l'écosystème cybercriminel.

Attaquant amateur

Source de risque

Les attaquants amateurs regroupent des individus disposant de compétences informatiques limitées à intermédiaires, souvent qualifiés de « script-kiddies ». Ces acteurs ne développent généralement pas leurs propres outils, mais utilisent des solutions disponibles en ligne, souvent prêtes à l'emploi.

Leur activité s'inscrit dans un contexte d'accessibilité croissante des outils offensifs, facilitée par la diffusion de kits d'attaque, de tutoriels et de plateformes spécialisées. Cette accessibilité réduit les barrières techniques et permet à un grand nombre d'individus de mener des attaques, même sans expertise approfondie.

Ces acteurs peuvent agir seuls ou au sein de petites communautés informelles, sans structure organisationnelle forte.

Objectifs visés

Les attaquants amateurs poursuivent principalement des objectifs relevant de la catégorie défi / amusement, telle que définie dans la méthode EBIOS Risk Manager.

Ces objectifs se traduisent par :

- Défi/Amusement (objectif principal)
  - tester leurs compétences techniques
  - relever un défi ou contourner des mécanismes de sécurité
  - obtenir une reconnaissance au sein d'une communauté
  - expérimenter des outils ou techniques d'attaque
- Lucratif (objectif secondaire, opportuniste)
  - exploitation opportuniste de vulnérabilités pour un gain ponctuel
  - participation indirecte à des activités frauduleuses

Ces motivations sont généralement peu structurées et peuvent évoluer rapidement en fonction des opportunités ou des intérêts individuels.

Motivation

Faible à modérée : motivations principalement liées à la curiosité, au défi ou à la reconnaissance, avec parfois des dérives opportunistes.

Ressources

Faibles : dépendance forte à des outils disponibles en ligne, peu de capacités de développement ou d'adaptation.

Activité

Élevée : grand nombre d'acteurs, réalisant des attaques fréquentes, souvent automatisées et opportunistes.

Modes opératoires

Les attaquants amateurs mettent en œuvre des attaques simples, généralement opportunistes :

- scans automatisés de systèmes exposés
- exploitation de vulnérabilités connues
- utilisation de scripts ou de kits d'attaque prêts à l'emploi
- tentatives d'accès non autorisé sur des services exposés

Ces attaques sont peu sophistiquées mais peuvent être efficaces en cas de défaut de configuration ou de vulnérabilités non corrigées.

Secteurs d'activité ciblés

Les attaquants amateurs ciblent de manière opportuniste :

- systèmes exposés sur Internet
- petites et moyennes entreprises
- organisations présentant des vulnérabilités connues

Dans le contexte d'Infrabel, ces acteurs peuvent cibler des systèmes exposés ou mal configurés, sans distinction particulière du secteur.

Arsenal d'attaque

- scripts d'exploitation disponibles en ligne
- scanners de vulnérabilités automatisés
- outils de brute force
- kits d'attaque accessibles publiquement

Faits d'arme

Les attaquants amateurs sont rarement associés à des attaques majeures. Leur impact se manifeste principalement par :

- un volume important de tentatives d'attaque ;
- des compromissions opportunistes de systèmes mal sécurisés ;

- une contribution indirecte à la pression globale sur les systèmes exposés.

Attaquant vengeur

Source de risque

Les attaquants vengeurs regroupent des individus animés par un sentiment d'injustice ou de frustration, généralement lié à une relation directe avec l'organisation ciblée. Il peut s'agir de salariés ou anciens salariés, de prestataires ou de partenaires ayant développé un ressentiment à l'égard de l'entité.

Ces acteurs se distinguent par leur connaissance interne des systèmes d'information, des procédures et des processus métier. Cette connaissance constitue un avantage majeur, leur permettant d'identifier des vulnérabilités spécifiques et de contourner certains mécanismes de sécurité.

Contrairement à d'autres profils, leur motivation est personnelle et émotionnelle, ce qui peut renforcer leur détermination et leur capacité à mener des actions ciblées.

Objectifs visés

Les attaquants vengeurs poursuivent principalement des objectifs relevant de la catégorie entrave au fonctionnement, telle que définie dans la méthode EBIOS Risk Manager.

Ces objectifs se traduisent par :

- Entrave au fonctionnement
  - perturbation des activités de l'organisation
  - sabotage de systèmes ou de processus internes
  - altération ou suppression de données
  - blocage ou dégradation des services
- Influence
  - atteinte à l'image de l'organisation
  - divulgation d'informations internes
  - volonté d'exposer des dysfonctionnements ou de nuire à la réputation.

Ces objectifs sont directement liés à une volonté de nuisance ciblée, souvent proportionnelle au ressentiment de l'attaquant.

Motivation

Élevée : motivation personnelle forte, souvent liée à un conflit ou un sentiment d'injustice. Peut conduire à des comportements déterminés et persistants.

Ressources

Faibles à modérées : niveau technique variable, mais compensé par une connaissance interne approfondie des systèmes et des processus.

Activité

Faible à modérée : actions généralement ponctuelles mais ciblées, pouvant avoir un impact significatif.

Modes opératoires

Les attaquants vengeurs mettent en œuvre des actions ciblées, souvent liées à leur connaissance interne :

- abus de droits ou de privilèges
- suppression ou altération de données
- sabotage de systèmes ou de procédures
- contournement de contrôles de sécurité
- divulgation d'informations internes

Ces actions sont généralement précises et orientées vers un impact direct.

Secteurs d'activité ciblés

Les attaquants vengeurs ciblent principalement leur propre organisation ou une entité avec laquelle ils ont eu une relation directe.

Dans le cas d'Infrabel, les risques concernent :

- les systèmes internes
- les procédures opérationnelles
- les données sensibles liées à l'exploitation ferroviaire

Arsenal d'attaque

- accès internes légitimes ou détournés
- outils internes
- scripts simples
- connaissances des systèmes et procédures

Faits d'arme

Les attaquants vengeurs sont rarement associés à des attaques médiatisées, mais leur impact peut être significatif :

- sabotage interne de systèmes
- suppression de données critiques
- divulgation d'informations sensibles

Ces incidents illustrent le risque élevé associé aux menaces internes.

Malveillant pathologique

Source de risque

Les malveillants pathologiques regroupent des individus dont les motivations sont d'ordre opportuniste, irrationnel ou parfois liées à l'appât du gain. Ce profil inclut notamment des concurrents déloyaux, des clients malhonnêtes, des fraudeurs ou des individus isolés agissant sans logique structurée.

Ces acteurs se caractérisent par un comportement imprévisible et une absence de stratégie claire. Leur niveau technique est variable : certains disposent de compétences suffisantes pour mener eux-mêmes des attaques, tandis que d'autres s'appuient sur des outils disponibles en ligne ou sous-traitent leurs actions à des officines spécialisées.

Cette combinaison d'opportunisme, de variabilité des moyens et d'imprévisibilité constitue un facteur de risque particulier, rendant leur détection et leur anticipation complexes.

Objectifs visés

Les malveillants pathologiques poursuivent des objectifs variés, relevant principalement des catégories lucratif et, dans certains cas, entrave au fonctionnement, telles que définies dans la méthode EBIOS Risk Manager.

Ces objectifs se traduisent par :

- Lucratif
  - fraude ou escroquerie
  - exploitation opportuniste de vulnérabilités
  - recherche de gain financier ponctuel
  - recours à des services externes pour mener des attaques
- Entrave au fonctionnement
  - perturbation opportuniste de systèmes ou de services
  - actions nuisibles sans objectif stratégique clair
  - exploitation de failles pour provoquer des dysfonctionnements

Contrairement à d'autres profils, ces objectifs ne s'inscrivent pas dans une logique structurée, mais résultent d'opportunités ou de motivations individuelles.

Motivation

Variable : motivations opportunistes, irrationnelles ou financières, sans cohérence stratégique. Peut inclure des comportements impulsifs.

Ressources

Faibles à modérées : dépend fortement de l'individu, avec possibilité de recours à des outils accessibles ou à des prestataires externes.

Activité

Faible à modérée : actions opportunistes, non systématiques, mais difficilement prévisibles.

Modes opératoires

Les malveillants pathologiques mettent en œuvre des actions opportunistes et hétérogènes :

- exploitation de vulnérabilités connues
- utilisation de kits d'attaque disponibles en ligne
- recours à des officines spécialisées
- fraude ou escroquerie numérique

- tentatives opportunistes de compromission

Ces attaques ne suivent pas nécessairement un schéma structuré et dépendent fortement des opportunités.

Secteurs d'activité ciblés

Les malveillants pathologiques ciblent de manière opportuniste :

- organisations accessibles ou vulnérables
- services exposés
- systèmes présentant des failles exploitables

Dans le cas d'Infrabel, les risques concernent principalement les systèmes exposés ou insuffisamment sécurisés.

Arsenal d'attaque

- outils disponibles en ligne
- kits d'attaque
- scripts simples
- services de piratage externalisés

Faits d'arme

Les actions des malveillants pathologiques sont rarement médiatisées, mais incluent :

- fraudes opportunistes
- exploitation de failles non corrigées
- attaques isolées sans coordination

Ces incidents illustrent une menace diffuse et difficile à anticiper.

CATALOGUES DES RISQUES

Les principaux rapports émis par les autorités nationales, agences européennes et parties prenantes de la Threat Intelligence révèlent une évolution des menaces, susceptibles d'impacter directement la continuité des services essentiels d'Infrabel, sa cyber résilience opérationnelle et la confiance de ses parties prenantes.

Dans ce contexte, Infrabel réalise régulièrement des analyses de risques s'appuyant sur la méthodologie EBIOS Risk Manager. Ces risques sont identifiés par consolidation des tendances dégagées dans des rapports de référence, puis traduits en enjeux métiers afin d'offrir une vision structurée, hiérarchisable et pertinente pour la prise de décision.

Les risques identifiés chez Infrabel sont aussi étroitement liés à la relation qu'elle entretient avec ses fournisseurs au sein de la supply chain. En effet, toute vulnérabilité ou incident affectant un fournisseur peut avoir un impact direct sur la sécurité et la continuité des services critiques d'Infrabel. Par exemple, une défaillance ou une cyberattaque chez un partenaire critique peut entraîner des perturbations majeures, voire compromettre la résilience opérationnelle de l'entreprise.

Inversement, les exigences et les pratiques de sécurité d'Infrabel influencent également les fournisseurs, qui doivent se conformer à des standards rigoureux pour assurer la fiabilité et la conformité réglementaire de l'ensemble de la supply chain.

Cette interdépendance souligne l'importance d'une gestion proactive des risques, basée sur une collaboration étroite et une évaluation continue des menaces et des faiblesses au sein du réseau de partenaires.

Risque	Définition
Interruption majeure de service essentiel	L'incapacité à assurer la continuité d'un ou plusieurs services critiques de la mission d'Infrabel représente un risque majeur pour l'organisation. Ce risque se traduit par une interruption des fonctions essentielles, mettant en péril la stabilité et la résilience opérationnelle de l'entreprise.
Défaillance critique liée à la Supply Chain	Un incident chez un fournisseur peut impacter directement l'activité, entraînant des perturbations significatives dans la chaîne d'approvisionnement et l'organisation opérationnelle.
Non-conformité réglementaire majeure	L'incapacité à respecter les exigences réglementaires représente un risque majeur pour l'organisation. Cette non-conformité peut avoir d'importantes conséquences, affectant la légitimité et la continuité des activités de l'entreprise. Il est donc essentiel de garantir le respect des obligations réglementaires afin de maintenir la conformité et d'assurer la pérennité de la mission.

Effet domino inter-infrastructures	Lorsqu'un incident survient dans une infrastructure critique, son impact peut rapidement se propager à d'autres secteurs essentiels. Ce phénomène de propagation, souvent qualifié d'effet domino, met en lumière la forte interdépendance entre différentes infrastructures. Ainsi, une perturbation initiale dans un secteur peut entraîner des conséquences majeures dans des domaines connexes, accentuant la gravité de la situation et la nécessité de disposer de mécanismes de gestion de crise adaptés.
Perte de contrôle des processus opérationnels / industriels	L'altération ou le pilotage malveillant des opérations physiques constitue un risque important pour les processus opérationnels ou industriels. Cette menace peut entraîner une perte de contrôle sur les activités, mettant en danger la sécurité et l'intégrité des systèmes concernés. Il est donc crucial de prévenir toute manipulation non autorisée afin de garantir le bon fonctionnement et la fiabilité des opérations.
Compromission de données sensibles ou stratégiques	L'exposition ou le vol de données critiques représente une menace majeure pour les infrastructures essentielles. La compromission de ces informations sensibles peut avoir des conséquences importantes, affectant la sécurité, la confidentialité et l'intégrité des secteurs concernés. Ce type d'incident souligne la nécessité de mettre en place des mesures robustes pour protéger les données stratégiques et limiter les impacts en cas de fuite ou d'accès non autorisé.
Altération de l'intégrité des données critiques	La manipulation discrète des données critiques représente une menace significative pour les organisations. Lorsqu'une altération cible ces informations, elle peut influencer les décisions prises au sein des processus opérationnels ou industriels. Ce risque découle du fait que des données falsifiées ou modifiées passent inaperçues, entraînant ainsi des choix ou des orientations qui ne reposent plus sur des informations fiables. La préservation de l'intégrité des données est donc essentielle pour garantir la pertinence et la sécurité des décisions stratégiques.
Extorsion à grande échelle	Les attaques par extorsion à grande échelle provoquent le blocage des systèmes informatiques, ce qui empêche les organisations d'accéder à leurs ressources essentielles. Ces incidents s'accompagnent généralement d'une forte pression financière et réputationnelle, poussant les victimes à répondre rapidement aux demandes des attaquants pour limiter les impacts sur leur activité et leur image publique.

Perte de confiance publique / institutionnelle	La perte de confiance publique ou institutionnelle se manifeste principalement par une dégradation de la crédibilité de l'entité concernée. Lorsqu'un incident de sécurité survient, qu'il s'agisse d'une altération des données ou d'une manipulation malveillante, la perception de fiabilité de l'organisation peut être rapidement compromise. La confiance accordée par les partenaires, les clients ou le grand public s'effrite, ce qui nuit durablement à l'image et à la réputation de l'institution. Ce phénomène constitue l'une des conséquences majeures des cybermenaces, car il fragilise non seulement les relations externes mais aussi la stabilité interne de l'entité.
Mise en danger de la vie humaine	Les incidents cyber peuvent avoir des conséquences physiques directes, mettant en danger la vie humaine. Lorsqu'un système critique est compromis, cela peut entraîner des dysfonctionnements ou des interruptions susceptibles d'impacter la sécurité des personnes concernées.
Dépendance critique à des systèmes non maîtrisés	La résilience d'une organisation peut être mise à mal en raison de sa dépendance à des systèmes technologiques qu'elle ne maîtrise pas totalement. Cette situation expose l'entité à des risques supplémentaires, car toute défaillance ou vulnérabilité affectant ces systèmes peut avoir des répercussions majeures sur son fonctionnement et sa capacité à faire face aux incidents.
Instrumentalisation dans un contexte géopolitique	L'entité peut être exploitée dans le cadre d'un contexte géopolitique, où elle sert de levier stratégique. Cela implique qu'elle soit utilisée par des acteurs cherchant à influencer ou à atteindre des objectifs politiques, économiques ou militaires, en profitant de sa position ou de ses capacités spécifiques.
Détection tardive d'un incident majeur	La présence prolongée d'un attaquant dans le système d'information constitue une situation où l'intrusion n'est pas détectée rapidement. Cela signifie qu'un individu malveillant peut rester dans l'environnement informatique de l'organisation sur une période étendue, ce qui augmente les risques et les conséquences potentielles pour la sécurité des données et le fonctionnement global de l'entité.
Incapacité à gérer une crise cyber majeure	La capacité de gérer une crise cyber majeure repose sur une organisation solide et des processus adaptés. Une défaillance dans la gestion organisationnelle de crise peut entraîner des conséquences importantes, notamment une réponse inefficace face à une attaque et une aggravation des impacts sur les activités critiques de l'entité. Il est donc essentiel que les structures et les procédures de crise soient clairement définies et régulièrement testées pour garantir leur efficacité en cas d'incident.

Perte de compétences critiques	La perte de compétences critiques peut survenir lorsque l'organisation repose fortement sur certains membres du personnel possédant des connaissances ou des expertises spécifiques. Cette dépendance à des ressources humaines clés expose l'entité à des risques accrus si ces personnes deviennent indisponibles, que ce soit de façon temporaire ou permanente. Une telle situation peut fragiliser la capacité de l'organisation à maintenir ses activités, à répondre efficacement à des incidents ou à assurer la continuité de ses opérations.

Au-delà de leur caractère générique, ces risques constituent une base essentielle pour la construction des scénarios stratégiques détaillés et leur déclinaison en scénarios opérationnels. Ils permettent également d'orienter les priorités en matière de gestion des risques, de résilience et de gouvernance de la sécurité.

Enfin, dans un environnement en constante évolution, cette analyse doit être régulièrement réévaluée afin d'intégrer les nouvelles tendances de la menace et les transformations du système d'information et des dépendances de l'entité.