niji x GROUPE Ovalt
Pour l'industrie de demain

LA DÉMARCHE SIMPLIFIÉE POUR LES INDUSTRIELS

CYBERSÉCURITÉ & NIS 2 : PAR OÙ COMMENCER ?

SOMMAIRE

01 Édito – NIS 2, un levier contre les risques de cybersécurité 01

02 Constat 2024 : un secteur industriel sous pression cyber 02

03 Directive NIS 2 : un tournant réglementaire pour l’industrie 04

04 Quelle approche terrain pour sécuriser vos usines ? 07

05 Conclusion : prendre le contrôle de sa cybersécurité OT 08

01.ÉDITO

Julien MOREL
Responsable de la Sécurité des Systèmes d'Information chez Ovalt

Pierre CORBEL
Directeur conseil Cybersécurité

La cybersécurité industrielle n'est plus une option.

La directive européenne NIS 2 impose à de nombreux industriels — qu'ils soient grands donneurs d'ordre ou acteurs de filières essentielles — de repenser leur protection face aux menaces numériques. Derrière cette obligation réglementaire, une réalité : les attaques ciblant l'OT se multiplient, exploitant des vulnérabilités souvent sous-estimées par les personnes en charge de ces systèmes. Pourtant, elles ont des impacts directs sur la production, la supply chain et parfois même la sécurité des collaborateurs.

C'est dans ce contexte qu'Ovalt et Niji ont décidé d'unir leurs expertises : l'une issue du terrain industriel et de l'intégration OT, l'autre ancrée dans la cybersécurité et la gouvernance. Ensemble, nous accompagnons les industriels pour transformer cette contrainte réglementaire en une véritable opportunité de mieux connaître leur existant, maîtriser leurs partenaires et bâtir une gouvernance cyber adaptée à leurs réalités opérationnelles.

Ce livre blanc a été conçu pour vous aider à franchir ce cap avec pragmatisme. Vous y trouverez notre approche pour : évaluer votre périmètre et votre niveau de conformité,

prioriser les actions sans céder aux sirènes de solutions miracles,

engager vos équipes — de la direction aux opérations — dans une démarche durable.

Nous sommes convaincus que la réussite repose sur une approche réaliste, progressive et partenariale. La cybersécurité industrielle ne s'impose pas d'en haut, elle se construit, étape par étape, au service de la continuité et de la performance des usines.

Le moment d'agir, c'est maintenant.

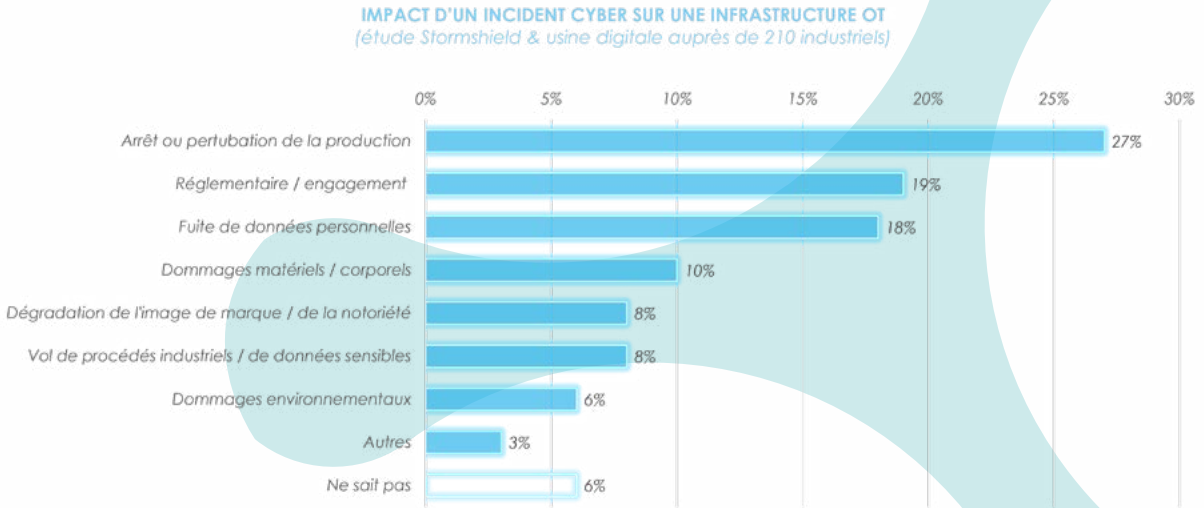
02. CONSTAT 2024 : UN SECTEUR INDUSTRIEL SOUS PRESSION CYBER

2.1 INDUSTRIE 4.0 ET MENACES CYBER

La cybersécurité industrielle entre dans une zone critique. Avec la transformation vers l'industrie 4.0, les environnements de production deviennent de plus en plus connectés (IoT, applications SaaS, accès à distance pour les prestataires) augmentant significativement la surface d'exposition aux risques.

Cette évolution rapide s'est faite sans toujours maîtriser la convergence Information Technology (Technologies de l'Information)/ Operational Technology (Technologies Opérationnelles), et dans un contexte où la maturité en cybersécurité OT reste encore trop faible.

La menace cyber n'est donc plus une hypothèse pour les industriels : elle est concrète, infiltrée jusque dans les ateliers, les lignes de production, les systèmes de supervision.



Impact d'un incident cyber sur une infrastructure
Source : Baromètre de la cybersécurité industrielle 2022 : Vers une prise en compte du risque au niveau de l'industrie du futur
Usine Digitale en collaboration avec Stormshield

2.2 LES ATTAQUES INDUSTRIELLES S'INVITENT DANS LES LIGNES

Les attaques contre les systèmes OT ne sont pas seulement de plus en plus fréquentes, elles sont également de mieux en mieux ciblées. Elles tirent parti de vulnérabilités propres aux environnements industriels, tels que des systèmes obsolètes non patchés, une segmentation réseau insuffisante, des accès VPN non sécurisés ou encore des prestataires externes insuffisamment contrôlés.

Quelques cas anonymisés illustrent l'impact de ces menaces

En mai 2025, une cyberattaque a paralysé une usine du secteur laitier, à la suite d'une **activité réseau suspecte**.

La production a été interrompue, provoquant des **retards de livraison** et nécessitant un redémarrage progressif via des **protocoles d'urgence**.

Aux États-Unis, en 2025, un acteur majeur de la sidérurgie a subi une **compromission de ses serveurs**, entraînant l'**arrêt immédiat** de **plusieurs sites de production**

La reprise s'est faite de manière progressive, avec des **impacts** sur la chaîne d'approvisionnement et des **retards clients**.

En 2022, un constructeur automobile japonais a été victime d'une **cyberattaque indirecte** via un fournisseur.

L'incident a conduit à l'**arrêt simultané de 14 usines**, perturbant fortement la supply chain et les plannings de livraison.

En 2021, une entreprise américaine de transformation de viande a été ciblée par un **ransomware touchant plusieurs sites**.

Deux usines ont été fermées temporairement, une **rançon** a été exigée, et la chaîne d'approvisionnement régionale a été perturbée.

Ce que ça révèle :

- Les attaques ciblent les **points faibles** : fournisseurs, accès distants, systèmes non mis à jour.
- L'impact est **systémique** : production, logistique, finance, RH sont affectés en cascade, sans oublier les clients finaux.
- Le facteur **temps est critique** : une attaque peut paralyser une usine en quelques heures et engendrer des pertes durables.

03. DIRECTIVE NIS 2 : UN TOURNANT RÉGLEMENTAIRE POUR L'INDUSTRIE

Qu'est-ce-que la directive NIS ?

Adoptée en 2016, la directive européenne NIS visait à renforcer la cybersécurité des services jugés essentiels au fonctionnement de l'économie et de la société. Face à l'évolution rapide des cybermenaces et aux limites de cette première version, une nouvelle directive, NIS 2, est publiée en 2022.

En France, l'ANSSI estime que le nombre d'entreprises concernées, directement ou indirectement, pourrait passer d'environ 300 « Opérateurs de services essentiels » (OSE) à près de 15 000 entités, tous secteurs confondus

L'objectif est clair : passer d'une cybersécurité ciblée à une cybersécurité de masse

La directive NIS 2 marque un changement d'échelle : il ne s'agit plus seulement de sécuriser les infrastructures critiques, mais d'intégrer l'ensemble des chaînes industrielles, sous-traitants inclus.

L'objectif est clair : passer d'une cybersécurité ciblée à une cybersécurité de masse, en responsabilisant un grand nombre d'acteurs face aux risques numériques.

Le socle de sécurité a été repensé pour faire face aux menaces actuelles, notamment celles liées aux fournisseurs ou à la dépendance technologique. L'harmonisation des exigences entre États membres vise à créer un cadre commun de résilience à l'échelle européenne.

L'impact sera-t-il le même pour l'ensemble des acteurs ?

En raison de l'augmentation significative du nombre d'entreprises concernées, la directive NIS 2 introduit le principe de proportionnalité dans l'application des mesures de cybersécurité ainsi que dans le régime de sanctions. Les exigences seront ainsi ajustées en fonction de la taille, du secteur et du niveau de risque propre à chaque entité.

Les organisations sont classées en deux catégories : Les entités essentielles et les entités importantes

Entités **E**ssentielles

Il s'agit ici des organisations dites «hautement critique». Le niveau d'exigence attendu sera le plus strict des deux catégories. Ici la gestion de la cybersécurité est capitale.

Entités **I**mportantes

Organisations importantes, mais dont l'impact est jugé moins «critique» : un socle de sécurité important leur sera appliqué, sans exiger le même niveau de maturité que les EE.

Champ d'application : qui est visé et dans quelle mesure ?

La réglementation identifie 18 secteurs d'activité, répartis en deux annexes, et fixe des critères de taille pour déterminer les entités concernées.

SECTEURS HAUTEMENT CRITIQUES :

Energie

Electricité | Gaz | Pétrole | Hydrogène | Réseaux de chaleur

Transport

Ferroviaire | Routier | Maritime | Aérien

Santé

Service des eaux

Eaux potables | Eaux usées

Secteur bancaire

Finance

Infra numérique

Service TIC

Administration publique

Espace

SECTEURS CRITIQUES :

Services postaux et expéditions

Gestion des déchets

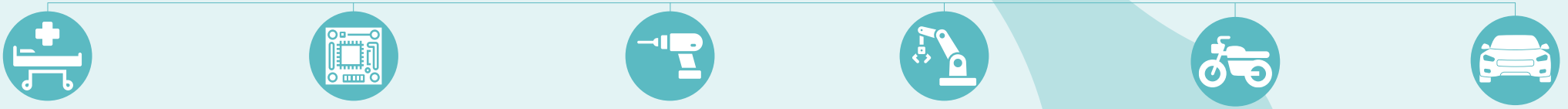
Produits chimiques

Denrées alimentaires

Recherche

Fournisseurs numériques

Fabrication



Dispostifis médicaux | Produits informatiques électroniques et optiques | Equipements électriques | Machines et équipements | Autres matériels de transport | Véhicules automobiles

Nouveaux secteurs concernés par la NIS 2

GROUPE Ovalt Pour l'industrie de demain

Mon organisation à :

- + de 250 salariés

ou

- Un C.A supérieur 50M€

ou

- un secteur hautement critique

Entités **E**ssentielles

Mon organisation à :

- + de 50 salariés

ou

- Un C.A supérieur 10M€

Entités **I**mportantes

Pour savoir si vous êtes concerné par NIS 2, nous vous invitons à aller sur http://monespacenis2.cyber.gouv.fr

Quelles sont les obligations pour les entités concernées ?

S'enregistrer à l'ANSSI	Les organisations concernées par la directive NIS 2 doivent s'identifier et se notifier auprès de l'ANSSI. Il est également demandé de fournir des points de contact désignés (comme le RSSI ou le responsable sécurité) et veiller à la mise à jour régulière de ces informations.
Gérer ses risques	Les entités devront mettre en œuvre des mesures juridiques, techniques et organisationnelles appropriées, en s'appuyant sur les objectifs de sécurité définis par l'ANSSI.
Déclaration d'incident	Tout incident majeur impactant l'activité de l'entreprise doit être signalé dans un délai de 72 heures.

Quelles sont les sanctions prévues en cas de non-respect de la norme ?

L'ANSSI est habilitée à réaliser des audits pour vérifier la conformité des organisations aux exigences de la directive NIS 2. En cas de manquement, les sanctions prévues sont comparables à celles du RGPD, et peuvent être à la fois financières et non financières.

Sanctions financières

- Entités Essentielles (EE) : jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu)

- Entités Importantes (EI) : jusqu'à 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial

Sanctions non financières

- Suspension temporaire ou définitive d'une certification de cybersécurité (EE)

- Suspension temporaire du droit d'exercer pour le dirigeant responsable (EE)

Source : Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 - NIS 2, Article 34
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555ritev5.2.pdf

GROUPE Ovalt
Pour l'industrie de demain

Quelles sont les mesures à mettre en place ?

La directive prévoit une vingtaine d'objectifs que l'on peut catégoriser en 4 parties.

Gouvernance

La gouvernance, qui s'intéresse à la gestion des risques, la connaissance du système d'information et de son écosystème.

Protection

La protection, qui s'intéresse aux mesures concrètes de sécurisation de votre système d'information. Ces mesures ont vocation à empêcher une attaque.

Résilience

La résilience, qui s'intéresse à la capacité de reprendre ou continuer une activité en cas d'attaque.

Défense

La défense, qui s'intéresse à la détection et la capacité de l'entreprise à réagir en cas d'attaque.

Source : ANSSI (2023) Référentiel de cybersécurité NIS 2 – Phase 3
https://www.lemagit.fr/rms/LeMagIT/NIS2-PROJETphase3decret20Reglesdesecuritev5.2.pdf

04. QUELLE APPROCHE TERRAIN POUR SÉCURISER VOS USINES

En tant qu'industriel, par quoi commencer ?

Avant toute chose, il est essentiel de réaliser un état des lieux de votre organisation. Cette phase initiale vous permettra d'établir une base solide pour structurer votre démarche de conformité à la directive NIS 2.

Trois axes sont à prendre en compte :

1. Se réapproprier son système d'information (SI)

Commencez par dresser un inventaire des actifs, cartographier les flux d'informations, identifier les interconnexions internes et externes : qui communique avec qui, et comment ?

«On ne protège que ce que l'on connaît.»

2. Identifier et évaluer les risques

Repérez les scénarios qui pourraient compromettre vos activités critiques. Cette étape est essentielle pour mettre en place des mesures de protection adaptées à votre réalité opérationnelle.

3. Évaluer votre niveau de conformité

Il est peu probable que vous partiez de zéro. Une auto-évaluation vous permettra de mesurer l'écart entre votre situation actuelle et les exigences de NIS 2. Cela vous aidera à définir les priorités.

(À noter : le guide des bonnes pratiques de l'ANSSI pour les environnements OT peut être un excellent point d'appui.)

Avec cette analyse, vous connaîtrez vos forces, vos faiblesses, les périmètres à sécuriser et surtout, vos priorités. L'objectif : construire une feuille de route claire, un plan d'action réaliste pour sécuriser vos systèmes d'information tout en respectant la réglementation.

Découvrez notre approche

De l'analyse de risques au diagnostic OT.

niji x GROUPE Ovalt Pour l'industrie de demain

05. CONCLUSION : PRENDRE LE CONTRÔLE DE SA CYBERSÉCURITÉ OT

Plan d'action : structurer et déployer votre démarche de cybersécurité OT

La suite dépendra de votre contexte propre — il n'existe pas de solution unique. Chaque entreprise possède ses spécificités, ses priorités et ses contraintes. Toutefois, à l'issue de votre plan d'action, vous serez en capacité de piloter avec assurance plusieurs volets clés de votre cybersécurité OT, notamment :

Une segmentation efficace de vos réseaux

Vous pourrez structurer vos systèmes d'information en zones distinctes afin d'appliquer des mesures de sécurité adaptées à chaque périmètre. Cela permet notamment de limiter les risques de propagation en cas d'attaque.

Une sensibilisation accrue de vos collaborateurs

Avec une politique de sensibilisation appropriée, vos équipes deviendront un maillon fort de votre cybersécurité. Sachant que 8 attaques sur 10 sont liées à une erreur humaine, la réduction de ce risque devient un levier majeur de protection.

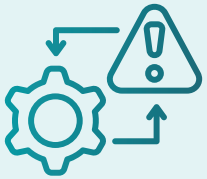
Une gouvernance claire de l'administration de vos SI

Vous saurez précisément qui administre quoi, comment et dans quel cadre. Cette maîtrise garantit une administration sécurisée et conforme aux exigences réglementaires.

Des capacités de détection d'intrusion sur votre SI

Grâce à des mécanismes de surveillance adaptés, vous serez en mesure de détecter et bloquer les intrusions avant qu'elles ne compromettent vos installations.

GROUPE Ovalt Pour l'industrie de demain



Une préparation solide à la gestion de crise

En cas d'incident, vous saurez qui mobiliser, comment communiquer en interne et à l'externe, et quelles actions enclencher pour contenir la situation et limiter les impacts.

Une continuité d'activité maîtrisée

Votre plan de continuité et de reprise d'activité vous permettra de redémarrer plus rapidement en cas de cyberattaque, avec des procédures claires, des interlocuteurs identifiés et des actions préalablement définies.

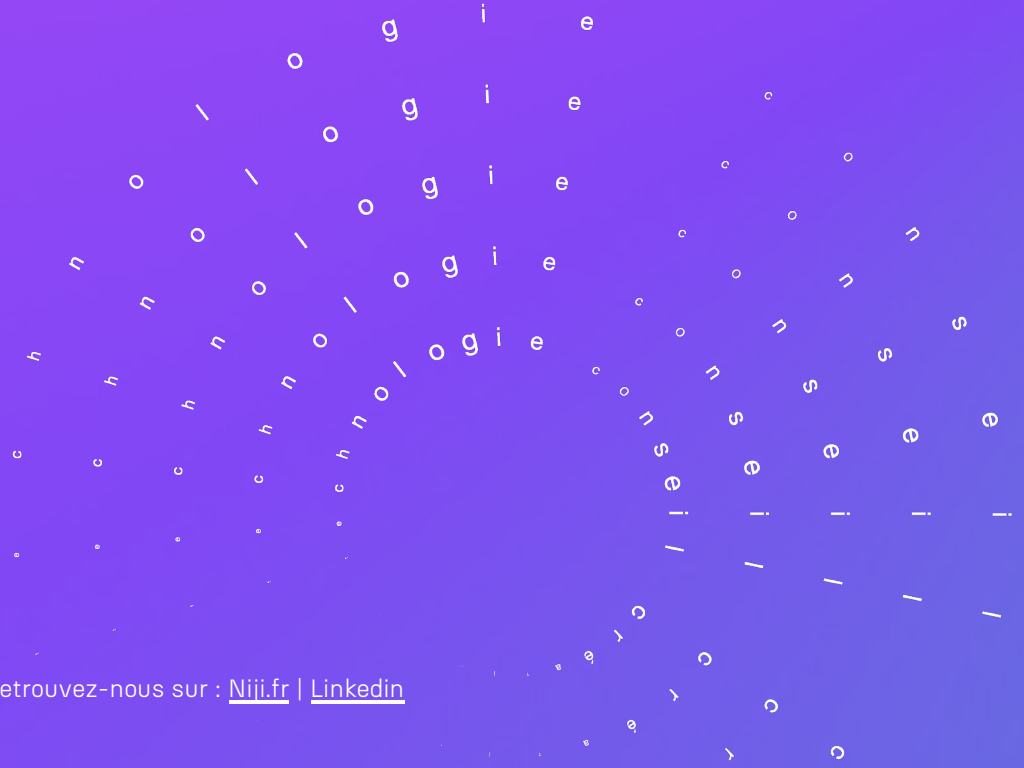
Une gestion proactive des risques

Vous disposerez d'une vision claire des vulnérabilités et des failles de vos systèmes, et pourrez engager des actions concrètes pour les traiter et réduire votre exposition aux menaces.

Et après cela ?

La cybersécurité n'est pas un projet ponctuel, mais une démarche continue. Elle se construit au quotidien, car vos systèmes d'information évoluent, tout comme les menaces et les vulnérabilités qui les ciblent. Pour rester efficace, la sécurité doit s'inscrire dans une logique d'amélioration continue, en phase avec votre contexte opérationnel et vos besoins métiers.

niji



Retrouvez-nous sur : Niji.fr | Linkedin

contact@niji.fr