AYI NEDJIMI Consultants

Conformité NIS 2 opérateurs importance vitale secteur OT

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide conformité NIS 2 pour les opérateurs d'importance vitale OT : obligations, mesures techniques, notification incidents et sanctions applicables.

Résumé exécutif

La directive européenne NIS 2, applicable depuis octobre 2024 et en cours de transposition dans les législations nationales, impose des obligations de cybersécurité considérablement renforcées aux entités essentielles et importantes exploitant des systèmes industriels dans les secteurs de l'énergie, des transports, de l'eau et de l'industrie manufacturière. Ce guide détaille les exigences spécifiques NIS 2 pour les opérateurs OT : les dix mesures de gestion des risques de l'article 21 appliquées aux systèmes de contrôle, le processus de notification des incidents en trois phases dans des délais stricts, la gouvernance renforcée avec responsabilité personnelle des dirigeants, la sécurisation de la chaîne d'approvisionnement incluant les fournisseurs d'automates, et les sanctions pouvant atteindre dix millions d'euros pour les entités essentielles en cas de non-conformité.

La directive NIS 2 (Network and Information Security Directive) représente un tournant réglementaire majeur pour la cybersécurité des systèmes industriels en Europe. Succédant à la directive NIS 1 de 2016, jugée insuffisante face à l'évolution des cybermenaces, NIS 2 élargit considérablement le périmètre des organisations concernées et renforce les obligations de sécurité et de notification. Les secteurs de l'énergie, des transports, de l'eau, de la santé, de la chimie et de l'industrie manufacturière sont explicitement couverts, ce qui inclut directement les systèmes de contrôle industriels de ces opérateurs dans le champ d'application de la directive. Pour les responsables de sécurité OT, NIS 2 transforme des bonnes pratiques recommandées en obligations légales assorties de sanctions financières significatives pouvant atteindre dix millions d'euros ou deux pourcent du chiffre d'affaires mondial pour les entités essentielles. Cette pression réglementaire, combinée à la menace croissante des cyberattaques contre les systèmes industriels critiques, crée un levier puissant pour débloquer les budgets de cybersécurité OT historiquement sous-dimensionnés et accélérer la mise en œuvre de mesures de protection attendues depuis des années par les équipes de sécurité des environnements de production industrielle.

Périmètre NIS 2 et classification des entités OT

NIS 2 distingue deux catégories d'entités soumises à des niveaux d'obligations différents. Les **entités essentielles** couvrent les secteurs de haute criticité : énergie (électricité, pétrole, gaz, hydrogène, chauffage/refroidissement), transports (aérien, ferroviaire, maritime, routier), eau

potable, eaux usées, infrastructures numériques et santé. Les **entités importantes** couvrent des secteurs complémentaires : industrie manufacturière, chimie, alimentation, gestion des déchets et services postaux.

Le critère de taille détermine l'applicabilité : les moyennes entreprises (50+ employés ou 10M+ CA) et grandes entreprises des secteurs couverts sont automatiquement soumises. Les *opérateurs d'importance vitale* (OIV) français, déjà soumis à la loi de programmation militaire (LPM), voient leurs obligations renforcées par NIS 2 sur certains aspects, notamment la gouvernance et la chaîne d'approvisionnement. La cartographie des systèmes OT dans le périmètre NIS 2 constitue la première étape de mise en conformité, en identifiant les systèmes d'information réseau industriels supportant les services essentiels fournis par l'organisation.

L'attaque ransomware contre le gestionnaire de pipeline Colonial Pipeline en mai 2021 a démontré les conséquences d'une cybersécurité insuffisante pour un opérateur d'infrastructure critique. L'absence de segmentation adéquate entre IT et OT, combinée à un manque de visibilité sur les systèmes industriels, a conduit à un arrêt préventif de six jours du principal pipeline de carburant de la côte Est américaine. Cet incident a accéléré les initiatives réglementaires aux États-Unis (directives TSA) et a renforcé la conviction européenne de la nécessité de NIS 2 pour imposer des standards minimaux de cybersécurité aux opérateurs d'infrastructures critiques.

Quelles mesures de gestion des risques NIS 2 pour les systèmes OT ?

L'article 21 de NIS 2 définit dix domaines de mesures de gestion des risques que les entités doivent mettre en œuvre. Leur application aux systèmes OT nécessite une interprétation adaptée aux contraintes industrielles. La **politique de sécurité** doit couvrir explicitement les systèmes de contrôle industriels avec des objectifs et des métriques adaptés (disponibilité plutôt que confidentialité). L'analyse de risque doit intégrer les spécificités OT : conséquences physiques, impact sur la sûreté des personnes, interdépendances entre systèmes de contrôle.

La **gestion des incidents** doit inclure des playbooks spécifiques OT prenant en compte les contraintes de disponibilité et de sûreté. La continuité d'activité doit couvrir les scénarios de compromission des systèmes de contrôle avec des procédures de passage en mode dégradé (commande manuelle). La sécurité de la *chaîne d'approvisionnement*, innovation majeure de NIS 2, s'étend aux fournisseurs d'automates, intégrateurs système et prestataires de maintenance OT. L'approche globale d'incident response doit intégrer ces exigences réglementaires. La sécurisation de la chaîne d'approvisionnement OT inclut l'évaluation des pratiques de cybersécurité des fabricants d'automates (certification IEC 62443-4-1), la vérification de l'intégrité des livraisons d'équipements et de logiciels (protection contre les attaques supply chain), et l'inclusion de clauses de cybersécurité dans les contrats avec les intégrateurs et mainteneurs ayant accès aux systèmes de contrôle industriels en production. Les fournisseurs critiques font l'objet d'audits périodiques validant le maintien de leur niveau de sécurité dans le temps, conformément aux exigences de diligence raisonnable de NIS 2.

Mesure NIS 2 (Art. 21)	Application OT	Priorité
Politique sécurité + analyse risque	IEC 62443 risk assessment	Haute
Gestion des incidents	Playbooks IR OT spécifiques	Haute
Continuité d'activité	Modes dégradés + PRA industriel	Haute
Sécurité chaîne approvisionnement	Audit intégrateurs + fournisseurs PLC	Moyenne
Sécurité acquisition/développement	IEC 62443-4-1 pour fournisseurs	Moyenne
Évaluation efficacité mesures	Pentest OT + exercices simulation	Moyenne
Cyber-hygiène + formation	Sensibilisation opérateurs OT	Haute
Cryptographie	Chiffrement communications OT critiques	Variable
Contrôle d'accès + gestion actifs	IAM OT + inventaire IACS	Haute
Authentification MFA	Accès distants OT + postes d'ingénierie	Haute

Mon avis : NIS 2 est la meilleure chose qui soit arrivée à la cybersécurité OT en Europe. Pendant des années, les responsables sécurité OT se sont heurtés au refus de budgets jugés non prioritaires par des directions focalisées sur la production. La perspective de sanctions financières de 10 millions d'euros et la responsabilité personnelle des dirigeants changent radicalement la dynamique budgétaire. NIS 2 ne résoudra pas tous les problèmes, mais elle force enfin les organisations à prendre la cybersécurité industrielle au sérieux et à allouer les ressources nécessaires.

Comment organiser la notification des incidents OT sous NIS 2 ?

NIS 2 impose un processus de notification en trois phases pour les incidents significatifs. L'**alerte précoce** doit être transmise au CSIRT national (CERT-FR en France) dans les 24 heures suivant la prise de connaissance de l'incident, incluant une indication sur l'origine potentiellement malveillante et l'impact transfrontalier éventuel. La **notification d'incident**, dans les 72 heures, détaille la nature de l'incident, sa sévérité, son impact et les mesures de remédiation en cours. Le **rapport final**, dans un délai d'un mois, fournit l'analyse complète incluant les causes racines et les leçons apprises.

Pour les incidents OT, la détermination du caractère « significatif » intègre des critères spécifiques : impact sur la fourniture du service essentiel (coupure électrique, interruption d'approvisionnement en eau), atteinte potentielle à la sûreté des personnes, et propagation possible à d'autres entités via les interconnexions industrielles. La mise en place de processus de notification fluides nécessite une coordination entre le SOC, les équipes OT, la direction juridique et les services de communication, formalisée dans des procédures testées lors d'exercices réguliers alignés sur les principes de détection et réponse aux incidents industriels.

Votre organisation a-t-elle testé sa capacité à notifier un incident OT significatif dans les 24 heures requises par NIS 2 ?

Pourquoi la gouvernance cyber OT est renforcée par NIS 2 ?

NIS 2 introduit une **responsabilité explicite des organes de direction** dans la gouvernance de la cybersécurité. Les dirigeants doivent approuver les mesures de gestion des risques, superviser leur mise en œuvre et suivre une formation en cybersécurité. Cette obligation s'étend aux systèmes OT : le directeur d'usine ou le directeur des opérations devient co-responsable de la sécurité des systèmes de contrôle industriels, ne pouvant plus déléguer intégralement cette responsabilité aux équipes IT.

Cette évolution de gouvernance nécessite la création d'un *comité de pilotage cybersécurité OT* réunissant la direction des opérations, la DSI, le RSSI et les responsables sûreté. Ce comité valide la stratégie de sécurité OT, arbitre les priorités entre production et sécurité, approuve les investissements nécessaires et supervise la mise en conformité. Les tableaux de bord de sécurité OT (taux de vulnérabilités critiques remédiées, couverture de surveillance réseau, résultats des exercices de simulation) alimentent les revues trimestrielles de ce comité. La structuration de cette gouvernance s'appuie sur l'architecture de SOC et supervision pour fournir les indicateurs nécessaires aux prises de décision.

Quelles sanctions en cas de non-conformité NIS 2 pour les opérateurs OT ?

Les **sanctions NIS 2** pour les entités essentielles peuvent atteindre 10 millions d'euros ou 2% du chiffre d'affaires mondial annuel. Pour les entités importantes, le plafond est de 7 millions d'euros ou 1,4% du CA mondial. Ces montants, significativement supérieurs aux sanctions NIS 1, sont complétés par des mesures de supervision renforcées incluant des audits imposés, des injonctions de mise en conformité et la possibilité de suspendre temporairement des certifications ou des autorisations d'exploitation.

La **responsabilité personnelle des dirigeants** constitue l'innovation la plus marquante de NIS 2 en termes de sanctions. Les personnes physiques responsables de la gouvernance de l'entité peuvent être tenues personnellement responsables en cas de manquement aux obligations de cybersécurité. Cette disposition vise à élever la cybersécurité au niveau de priorité de la direction générale, au même titre que la sécurité financière ou la conformité réglementaire. Pour les opérateurs OT, cette responsabilité inclut les décisions relatives à la sécurité des systèmes de contrôle industriels, renforçant l'urgence de la mise en conformité des environnements de production. Les autorités nationales de supervision disposent également du pouvoir d'imposer des mesures correctives immédiates, incluant des restrictions opérationnelles, en cas de risque imminent pour la sécurité des systèmes de contrôle industriels des entités essentielles et importantes soumises à NIS 2. L'alignement avec la directive NIS 2 dans sa dimension globale guide cette mise en conformité structurante.

Sources et références : CISA ICS · ANSSI

Faut-il utiliser IEC 62443 pour démontrer la conformité NIS 2 ?

La norme **IEC 62443** constitue le référentiel technique le plus pertinent pour démontrer la conformité des systèmes OT aux exigences de l'article 21 de NIS 2. Le mapping entre les mesures NIS 2 et les parties de l'IEC 62443 montre une correspondance étroite : l'analyse de risque NIS 2 s'appuie sur l'IEC 62443-3-2, les mesures de sécurité technique sur l'IEC 62443-3-3, et les exigences de développement sécurisé sur l'IEC 62443-4-1. Les organismes de certification comme IEC et TÜV facilitent cette démonstration par des certifications reconnues internationalement.

Les rapports de Dragos sur l'état de la sécurité OT fournissent des benchmarks sectoriels utiles pour évaluer la maturité de conformité. La combinaison IEC 62443 + ISO 27001 couvre l'ensemble des exigences NIS 2 pour les organisations exploitant des systèmes industriels. ISO 27001 adresse les aspects organisationnels (SMSI, gestion des risques, formation, audit) tandis qu'IEC 62443 couvre les spécificités techniques OT (zones et conduits, Security Levels, sécurité des composants). Cette approche duale permet de capitaliser sur les certifications existantes tout en répondant aux exigences spécifiques des systèmes de contrôle industriels. L'investissement dans les pratiques de threat hunting OT et de détection proactive démontre une maturité de sécurité allant au-delà de la simple conformité réglementaire et renforce la posture défensive globale de l'organisation face aux cybermenaces ciblant les infrastructures industrielles critiques.

À retenir : NIS 2 transforme la cybersécurité OT d'une bonne pratique recommandée en obligation légale assortie de sanctions significatives. La mise en conformité des systèmes industriels s'appuie sur IEC 62443 pour les mesures techniques et ISO 27001 pour la gouvernance. La responsabilité personnelle des dirigeants et les sanctions financières élevées créent le levier nécessaire pour débloquer les investissements en cybersécurité OT historiquement sous-dimensionnés.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr