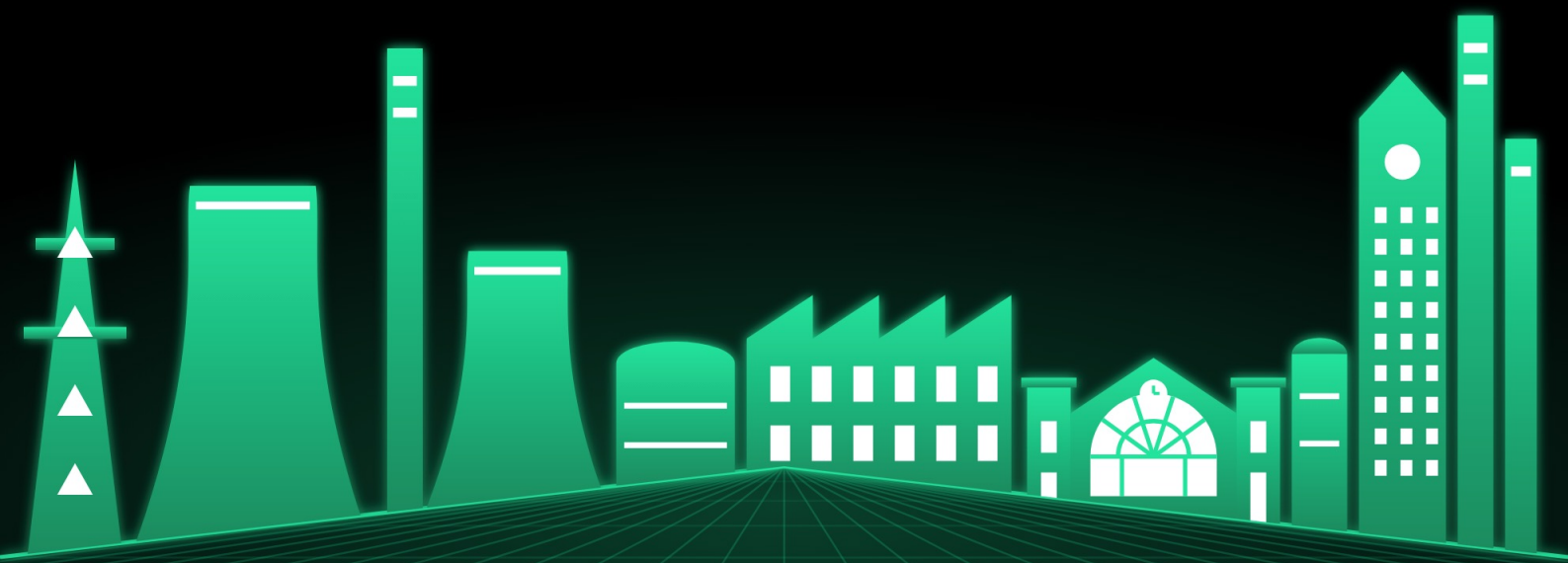
seclab.

GUIDE PRATIQUE · CYBERSÉCURITÉ INDUSTRIELLE

NIS 2 et ReCyF appliqués à l'industrie

Qui est concerné, quels objectifs atteindre et comment protéger vos systèmes industriels sans arrêter la production.



SOMMAIRE

Dans ce guide

01 **Comprendre**
NIS 2 et ReCyF en quelques mots 3

02 **Qui est concerné ?**
Votre organisation est-elle concernée ? 4
Entité essentielle ou importante : ce qui change 5

03 **Les objectifs du ReCyF**
4 piliers pour couvrir la cybersécurité 6
Les objectifs en bref 7

04 **Les spécificités de l'OT**
Appliquer le ReCyF sans perturber la production 9

05 **Comment Seclab vous aide**
Découvrir, isoler, détecter 10
Seclab et le ReCyF 11
Toutes les mesures couvertes 12

Les sigles de ce guide

SI	Système d'information	**OT**	Technologies opérationnelles (automates, réseaux industriels)
NIS 2	Directive européenne (UE) 2022/2555 sur la cybersécurité	**ReCyF**	Référentiel Cyber France publié par l'ANSSI
ANSSI	Agence nationale de la sécurité des systèmes d'information	**EE / EI**	Entité essentielle / entité importante
EDR	Détection et réponse sur les postes et serveurs	**SOC / SIEM**	Centre de supervision de la sécurité / outil de centralisation des journaux
PCA / PRA	Plans de continuité et de reprise d'activité	**EBIOS RM**	Méthode d'analyse de risques de l'ANSSI
MCO / MCS	Maintien en conditions opérationnelles et de sécurité	**MVDI**	Périmètre des actifs vitaux à la continuité (page 10)

Ce guide est fourni à titre informatif et ne constitue pas un avis juridique. Il s'appuie sur la directive (UE) 2022/2555 et sur le ReCyF v2.5 publié par l'ANSSI le 17 mars 2026, document de travail susceptible d'évoluer avec la loi de transposition. Reportez-vous aux textes officiels et à l'ANSSI pour déterminer vos obligations.

NIS 2 et ReCyF en quelques mots

La directive européenne NIS 2 élève le niveau de cybersécurité attendu de milliers d'organisations. En France, l'ANSSI en décline les exigences dans un référentiel concret : le ReCyF.

LA DIRECTIVE NIS 2

La directive (UE) 2022/2555, dite NIS 2, remplace la directive NIS de 2016. Elle change d'échelle : **18 secteurs** et, selon l'ANSSI, on passe de quelques centaines d'entités désignées à **environ 15 000 entités** concernées en France.

Trois obligations principales :

- **S'enregistrer** auprès de l'ANSSI
- **Gérer les risques cyber** avec des mesures techniques et organisationnelles
- **Notifier les incidents importants** : alerte précoce sous 24 h, notification sous 72 h, rapport final sous un mois

Les dirigeants approuvent les mesures et en répondent. Les sanctions peuvent atteindre **10 M€ ou 2 %** du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

LE RÉFÉRENTIEL ReCyF

Le **Référentiel Cyber France**, publié par l'ANSSI le 17 mars 2026 (version 2.5), décline les exigences de NIS 2 en **20 objectifs de sécurité**.

Quoi ?
L'**objectif de sécurité** fixe l'obligation à atteindre.

Comment ?
Les **moyens acceptables de conformité** proposent des mesures concrètes. Facultatifs, ils permettent de démontrer sa conformité en cas de contrôle.

Le référentiel est **proportionné** : 15 objectifs pour toutes les entités, 5 de plus pour les entités essentielles. Certaines certifications (ISO 27001) et prestations qualifiées par l'ANSSI aident à démontrer la conformité.

Les grandes dates

2016
Directive NIS

Déc. 2022
Publication de NIS 2

Oct. 2024
Date limite de transposition par les Etats membres

Mars 2026
L'ANSSI publie le ReCyF

Oct. 2026
Loi de transposition toujours en attente de vote en France

Faut-il attendre la loi ? Non. Le ReCyF reste un document de travail tant que la loi « Résilience » n'est pas adoptée. L'examen à l'Assemblée nationale a encore été reporté en octobre 2026, mais l'ANSSI encourage les entités à appliquer le référentiel dès maintenant. Engager la démarche dès aujourd'hui, c'est prendre de l'avance sur les contrôles.

Votre organisation est-elle concernée ?

Le **secteur d'activité** et la **taille** de l'entreprise permettent de répondre

1 Votre secteur fait-il partie des 18 secteurs visés ?

Secteurs hautement critiques (annexe I)

- Énergie
- Transports
- Banques
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructures numériques
- Services TIC (B2B)
- Administrations publiques
- Espace

Autres secteurs critiques (annexe II)

- Services postaux
- Gestion des déchets
- Produits chimiques
- Alimentation
- Fabrication
- Fournisseurs numériques
- Recherche

2 Croisez avec votre taille

	Petite moins de 50 salariés et CA ⩽ 10 M€	Moyenne 50 salariés ou plus ou CA > 10 M€	Grande 250 salariés ou plus ou CA > 50 M€
Secteur hautement critique	Non concernée	EI Entité importante	EE Entité essentielle
Autre secteur critique	Non concernée	EI Entité importante	EI Entité importante
Télécoms, services de confiance, DNS, État central[1]	EE / EI selon l'activité	EE / EI selon l'activité	EE Entité essentielle

[1] Toujours EE : prestataires de services de confiance qualifiés, registres de noms de domaine, fournisseurs DNS, administrations centrales. Télécoms : EI s'ils sont petits, EE dès la taille moyenne. Seuils simplifiés : la taille tient compte de l'effectif, du chiffre d'affaires, du bilan et des entreprises liées.

Pour confirmer votre statut, faites le test d'éligibilité de l'ANSSI sur messervices.cyber.gouv.fr/nis2, qui permet aussi de se pré-enregistrer. Les seuils du visuel sont volontairement simplifiés : en cas de doute (groupe, filiale, activité mixte), fiez-vous à ce test.

Entité essentielle ou importante : ce qui change

Les deux catégories ont les **mêmes obligations de fond**. Ce qui les distingue, c'est le nombre d'objectifs à atteindre, la manière dont l'autorité les contrôle et le plafond des sanctions.

	Entité essentielle (EE)	Entité importante (EI)
Qui ?	Grandes entités des secteurs hautement critiques, et certaines activités quelle que soit leur taille (DNS, registres, prestataires de confiance qualifiés, administrations centrales)	Entités moyennes des secteurs hautement critiques, entités moyennes et grandes des autres secteurs critiques
Obligations	S'enregistrer, gérer les risques cyber, notifier les incidents importants	Identiques
Objectifs du ReCyF	Les 20 objectifs, avec des moyens de conformité plus exigeants	Les objectifs 1 à 15
Supervision	A priori : l'autorité peut contrôler à tout moment (inspections, audits, scans de sécurité)	A posteriori : contrôles déclenchés par un indice de manquement ou un incident
Sanctions maximales	10 M€ ou 2 % du CA annuel mondial	7 M€ ou 1,4 % du CA annuel mondial

Exemples d'exigences propres aux entités essentielles

- **Authentification multifacteur** pour les accès distants (mesure 8.3)
- **Équipements personnels interdits** sur les systèmes d'information (mesure 9.2)
- **Plans de continuité et de reprise** adaptés aux crises cyber (mesure 13.6)
- **Analyse de risques** de chaque système (objectif 16)
- **Programme d'audits** de sécurité (objectif 17)
- **Supervision de la sécurité** avec traitement des événements sous 24 h (objectif 20)

4 piliers pour couvrir la cybersécurité

L'ANSSI regroupe les 20 objectifs dans quatre piliers, de l'organisation à la gestion de crise. Les objectifs marqués **EE** ne concernent que les entités essentielles.

Gouvernance

Savoir ce que l'on protège et piloter

- 1. Recensement des systèmes d'information
- 2. Cadre de gouvernance de la sécurité numérique
- 3. Maîtrise de l'écosystème
- 4. Sécurité numérique dans la gestion des RH
- 5. Maîtrise des systèmes d'information
- 16. Mise en œuvre d'une approche par les risques **EE**
- 17. Audit de la sécurité des systèmes d'information **EE**

Protection

Cloisonner, contrôler, durcir

- 6. Maîtrise des accès physiques aux locaux
- 7. Sécurisation de l'architecture des SI
- 8. Sécurisation des accès distants aux SI
- 9. Protection des SI contre les codes malveillants
- 10. Gestion des identités et des accès des utilisateurs
- 11. Maîtrise de l'administration des SI
- 18. Sécurisation de la configuration des ressources **EE**
- 19. Administration depuis des ressources dédiées **EE**

Défense

Détecter et superviser

- 12. Identification et réaction aux incidents de sécurité
- 20. Supervision de la sécurité des systèmes d'information **EE**

Résilience

Sauvegarder, gérer la crise, s'entraîner

- 13. Continuité et reprise d'activité
- 14. Réaction aux crises d'origine cyber
- 15. Exercices, tests et entraînements

Ce qui aide à démontrer la conformité

Le ReCyF (v2.5) précise, objectif par objectif, la certification et les prestations qualifiées par l'ANSSI dont une entité peut se prévaloir lors d'un contrôle pour démontrer qu'elle respecte l'objectif.

ISO 27001	SMSI certifié ISO/CEI 27001:2022, sur les SI couverts par la certification	Objectifs 2 et 16
PACS	Accompagnement et conseil en sécurité	Objectifs 12, 14, 15 et 16
PASSI	Audit de la sécurité des SI	Objectif 17
PAMS	Administration et maintenance sécurisées	Objectif 19 (9 mesures sur 12)
PDIS	Détection des incidents de sécurité	Objectif 20 (une partie des mesures)

Ressources officielles

- **Test d'éligibilité et pré-enregistrement** : messervices.cyber.gouv.fr/nis2
- **ReCyF** et outil de comparaison avec d'autres référentiels, publiés par l'ANSSI
- **Dossier NIS 2 de l'ANSSI** : cyber.gouv.fr
- **Directive (UE) 2022/2555** : eur-lex.europa.eu

Les objectifs en bref : organiser et tenir

Gouvernance



1 Recensement des systèmes d'information EI · EE

Lister ses activités, ses services et les systèmes d'information qui les supportent. Justifier les systèmes exclus du périmètre.



2 Cadre de gouvernance de la sécurité numérique EI · EE

Mettre en place une organisation, des rôles et une politique de sécurité approuvée par le dirigeant. Analyser sa conformité et suivre un plan d'action.



3 Maîtrise de l'écosystème EI · EE

Cartographier prestataires, fournisseurs et interconnexions. Inscrire les exigences de sécurité dans les contrats et les vérifier.



4 Sécurité numérique dans la gestion des RH EI · EE

Charte d'usage opposable, sensibilisation de tous, formation des fonctions numériques, gestion des arrivées et des départs.



5 Maîtrise des systèmes d'information EI · EE

Tenir une cartographie à jour, assurer une veille sur les vulnérabilités, appliquer les correctifs et atténuer le risque des systèmes non patchables.



16 Mise en œuvre d'une approche par les risques EE

Analyser les risques de chaque système (la méthode EBIOS RM est possible), accepter les risques résiduels et réexaminer au moins tous les trois ans.



17 Audit de la sécurité des systèmes d'information EE

Programme d'audits (test d'intrusion, configuration, architecture, organisation) et plan de correction des écarts constatés.

Résilience



13 Continuité et reprise d'activité EI · EE

Sauvegardes protégées et testées au moins une fois par an. Pour les EE, plans de continuité et de reprise d'activité.



14 Réaction aux crises d'origine cyber EI · EE

Procédure de crise, liste papier des personnes mobilisables, annuaire des parties prenantes. Pour les EE, retours d'expérience et communication de crise.



15 Exercices, tests et entraînements EI · EE

Entraîner régulièrement la cellule de crise, au minimum par un exercice sur table. Pour les EE, programme d'exercices sur trois ans.

Les objectifs en bref : protéger et détecter

Protection



6 Maîtrise des accès physiques aux locaux EI · EE

Contrôler l'accès aux locaux, aux salles serveurs et aux locaux techniques, et encadrer les visiteurs.



7 Sécurisation de l'architecture des SI EI · EE

Cloisonner les systèmes, n'autoriser que les interconnexions nécessaires et filtrer les flux avec un blocage par défaut.



8 Sécurisation des accès distants aux SI EI · EE

Chiffrer les accès effectués depuis l'extérieur et les authentifier. Authentification multifacteur pour les entités essentielles.



9 Protection des SI contre les codes malveillants EI · EE

Maîtriser les équipements et supports amovibles connectés, analyser les données venant de l'extérieur et déployer antivirus ou EDR.



10 Gestion des identités et des accès des utilisateurs EI · EE

Comptes individuels, secrets robustes changés à la mise en service, droits limités au strict besoin et revus chaque année.



11 Maîtrise de l'administration des SI EI · EE

Utiliser des comptes dédiés à l'administration. Pour les EE, sécuriser l'administration des annuaires (cœur de confiance).



18 Sécurisation de la configuration des ressources EE

Réduire la surface d'attaque : uniquement les logiciels nécessaires, configuration durcie et revue annuelle.



19 Administration depuis des ressources dédiées EE

Administrer depuis des postes et un réseau dédiés, avec des flux d'administration chiffrés et cloisonnés.

Défense



12 Identification et réaction aux incidents de sécurité EI · EE

Se doter d'une organisation, de processus et d'outils pour qualifier et traiter les incidents, et conserver les preuves techniques.



20 Supervision de la sécurité des systèmes d'information EE

Collecter et traiter journaux et événements sous 24 h, améliorer la détection en continu et conserver les traces au moins trois mois.

Appliquer le ReCyF sans perturber la production

Les technologies opérationnelles (OT) obéissent à d'autres règles que l'informatique de gestion : la disponibilité et la sûreté passent avant tout.

La disponibilité d'abord
Obj. 2 · 16

Une mesure de sécurité peut perturber la sûreté ou la continuité de production

Observer sans perturber
Obj. 1 · 3 · 5

Cartographie et inventaire passifs, non intrusifs

Des actifs figés
Obj. 5 · 9

OS obsolètes, équipements non patchables : des mesures compensatoires nécessaires

Patcher au rythme de l'usine
Obj. 5

Correctifs appliqués lors des arrêts de maintenance programmés

Des protections qui vieillissent
Obj. 5 · 9

Équipements isolés ou mobiles : correctifs et signatures en retard

Des portes dérobées
Obj. 3 · 8 · 9

Prestataires, routeurs 4G, clés USB : des accès à cartographier

Des responsables métier
Obj. 1 · 4

Les actifs sont gérés par des automaticiens, pas par l'IT

Une criticité contextuelle
Obj. 1 · 16

La criticité d'un actif dépend du process qu'il pilote

Le référentiel a prévu ces situations

- Quand un correctif est impossible, le ReCyF demande des **mesures d'atténuation** et cite l'exemple d'« isoler la ressource du reste du SI » (mesure 5.B.6).
- Pour les supports USB, il cite un « **SAS de décontamination** » (mesure 9.7).
- Une mesure alternative reste possible si elle est **justifiée** dans l'analyse de conformité (mesure 2.C.3).

Cinq réflexes pour l'OT

1. **Observer avant d'agir** : une cartographie passive ne perturbe pas les procédés.
2. **Isoler ce qui ne peut pas être patché**, plutôt que d'attendre une mise à jour qui ne viendra pas.
3. **Privilégier une protection matérielle plutôt que logicielle** : sans mise à jour à appliquer, le niveau de sécurité se maintient dans le temps.
4. **Choisir des solutions qui parlent aussi le langage des automaticiens** et des responsables d'usine, pas seulement celui de l'IT.
5. **Mettre les responsables métier dans la boucle** : la criticité d'un actif dépend du process qu'il pilote.

Découvrir, isoler, détecter

Seclab Xcore est la seule plateforme européenne de cybersécurité OT qui combine découverte, isolation et détection. Elle accompagne la mise en conformité étape par étape, au rythme de vos cycles industriels.

Découvrir 1

Xplore

Cartographie non-intrusive : inventaire des actifs, vues métier, matrice des flux réellement observés, vulnérabilités, criticité des actifs, identification des accès distants et usages USB. On ne protège bien que ce que l'on connaît.

Objectifs ReCyF : 1, 3, 5, 7, 8, 9, 17, 18

Isoler 2

Xchange Xport

Xchange cloisonne physiquement les réseaux par rupture protocolaire matérielle (Electronic AirGap). Xport agit comme un firewall USB. Il isole les ports USB et ne laisse passer que les fichiers analysés et signés par une station blanche.

Objectifs ReCyF : 5, 7, 8, 9, 11, 12, 13, 14, 19, 20

Détecter 3

Xplore

Quatre moteurs de détection complémentaires dont une augmentée par l'IA, identification des écarts par rapport à la baseline ou des anomalies opérationnelles, alertes contextualisées et intégration native avec votre SOC ou votre SIEM.

Objectifs ReCyF : 12, 20

MVDI

Minimum Viable Digital Industry

Le périmètre des actifs vitaux à la continuité de l'entreprise, isolé en priorité avec le plus haut niveau de sécurité. Hors de ce périmètre, une segmentation classique suffit.

Électronique, pas logiciel

Aucune session réseau ne traverse la passerelle : pas de reconnaissance, pas de mouvement latéral, résistance aux attaques zero-day et aux évasions d'agent IA.

Peu de maintenance

Pas de patch management pour appliquer des correctifs sur les produits d'isolation, environ une mise à jour fonctionnelle par an.

Souverain

Capital 100 % européen, conception et assemblage en France. Technologie Electronic AirGap certifiée CSPN par l'ANSSI.

seclab.

Par où commencer ?

Un audit Xplore de quelques heures, en écoute passive, donne un inventaire complet, la cartographie de vos flux et une première liste de vulnérabilités. L'audit réalisé permet d'identifier le périmètre à sécuriser et constitue la base de votre dossier de conformité.

seclab-security.com · contact@seclab-security.com

Seclab et le ReCyF

Nous avons rapproché chaque mesure du ReCyF des capacités de la plateforme Xcore : **14 objectifs sur 20** sont adressés, à travers **43 mesures**.

Objectif de sécurité	Mesures couvertes	Produits Seclab
1. Recensement des systèmes d'information	1 / 3	Xplore
2. Cadre de gouvernance de la sécurité numérique	0 / 11	—
3. Maîtrise de l'écosystème	1 / 4	Xplore
4. Sécurité numérique dans la gestion des RH	0 / 5	—
5. Maîtrise des systèmes d'information	5 / 10	Xplore Xchange Xport
6. Maîtrise des accès physiques aux locaux	0 / 4	—
7. Sécurisation de l'architecture des SI	13 / 13	Xplore Xchange Xport
8. Sécurisation des accès distants aux SI	1 / 5	Xplore Xchange
9. Protection des SI contre les codes malveillants	6 / 7	Xplore Xport
10. Gestion des identités et des accès des utilisateurs	0 / 17	—
11. Maîtrise de l'administration des SI	1 / 14	Xchange
12. Identification et réaction aux incidents de sécurité	3 / 7	Xplore Xchange
13. Continuité et reprise d'activité	1 / 7	Xchange
14. Réaction aux crises d'origine cyber	1 / 10	Xport
15. Exercices, tests et entraînements	0 / 4	—
16. Mise en œuvre d'une approche par les risques EE	0 / 4	—
17. Audit de la sécurité des systèmes d'information EE	1 / 5	Xplore
18. Sécurisation de la configuration des ressources EE	1 / 4	Xplore
19. Administration depuis des ressources dédiées EE	2 / 12	Xchange
20. Supervision de la sécurité des systèmes d'information EE	6 / 6	Xplore Xchange

Lecture. Une mesure est comptée dès qu'un produit Xcore y répond : directement (21 mesures, cœur de l'offre) ou en partie (22 mesures). Sur ces 43 mesures, 20 concernent aussi les entités importantes. Les objectifs non couverts relèvent surtout de l'organisation et d'autres outils, auxquels Xcore s'intègre (SIEM, SOC, bastion, pare-feu).

Toutes les mesures couvertes

Le détail des 43 mesures du ReCyF auxquelles la plateforme Xcore répond, objectif par objectif.

Mesure	Ce que demande le ReCyF	La réponse Seclab
1 Recensement des systèmes d'information		
1.1 EI · EE	Lister l'ensemble des activités/services et les systèmes d'information les supportant.	**Xplore** Contribution Inventaire exhaustif et exportable des actifs OT, y compris les équipements oubliés ou inconnus (shadow assets). Xplore fournit la matière première de la liste exigée.
3 Maîtrise de l'écosystème		
3.A.1 EI · EE	Cartographie de l'écosystème incluant la liste des interconnexions avec les SI de l'entité.	**Xplore** Contribution Cartographie des flux reels. Xplore révèle les interconnexions avec les prestataires ou fournisseurs non documentées.
5 Maîtrise des systèmes d'information		
5.A.1 EI · EE	Cartographie suffisante pour le MCO/MCS et la réaction à incident (identifier les ressources vulnérables ou affectées).	**Xplore** Cœur d'offre Cartographie multi-vues automatique (actifs, flux, vulnérabilités) ; identification immédiate des ressources concernées par un bulletin d'alerte ou un incident (et des responsables opérationnels de ces ressources).
5.B.3 EI · EE	Veille sur les vulnérabilités et correctifs de sécurité	**Xplore** Cœur d'offre Inventaire des vulnérabilités
5.B.6 EI · EE	Mesures d'atténuation quand l'installation des correctifs est impossible. Exemple cité : « isoler la ressource du reste du SI ».	**Xchange** **Xport** Cœur d'offre L'isolation matérielle est l'exemple donné par le référentiel. Xport apporte une réponse adaptée de sécurité pour le parc legacy OT non patchable.
5.B.8 EI · EE	Vérifier que les logiciels et mises à jour proviennent des ressources officielles.	**Xport** Contribution Contrôle d'accès par signature cryptographique des fichiers et mises à jour introduits dans l'environnement OT.
5.B.9 EI · EE	Réduction du risque lié à l'utilisation de versions obsolètes / non supportées.	**Xchange** - **Xport** Cœur d'offre Confinement matériel des équipements en fin de support (Windows XP, OS propriétaires) sans arrêt de production.
7 Sécurisation de l'architecture des SI		
7.A.1 EI · EE	Cloisonnement physique et/ou logique de l'ensemble des SI vis-à-vis des SI tiers et des SI hors périmètre.	**Xchange** - **Xport** Cœur d'offre Cloisonnement PHYSIQUE par Electronic AirGap. Le cloisonnement reste efficace dans le temps, sans nécessiter de correctifs.
7.A.2 EE	Cloisonnement de chaque SI vis-à-vis des autres SI.	**Xplore** - **Xchange** - **Xport** Cœur d'offre Identification des SI et de leurs liens. Isolation matérielle SI par SI sur le périmètre critique (approche MVDI : Minimum Viable Digital Industry).
7.A.3 **7.A.4** EE	Définir des sous-systèmes homogènes et les cloisonner entre eux.	**Xplore** - **Xchange** - **Xport** Cœur d'offre Xplore objective le découpage en sous-systèmes (zones / conduits type IEC 62443) ; Xchange et Xport les cloisonnent physiquement.
7.A.5 **7.A.6** EE	Passerelles sortante et entrante : authentifier, filtrer et tracer les accès vers/depuis les SI tiers.	**Xchange** Contribution Passerelle à rupture protocolaire (proxys TCP, UDP, FTP, FTPS, SFTP) pouvant être utilisée en double barrière, avec traçabilité native des échanges.

Toutes les mesures couvertes (suite)

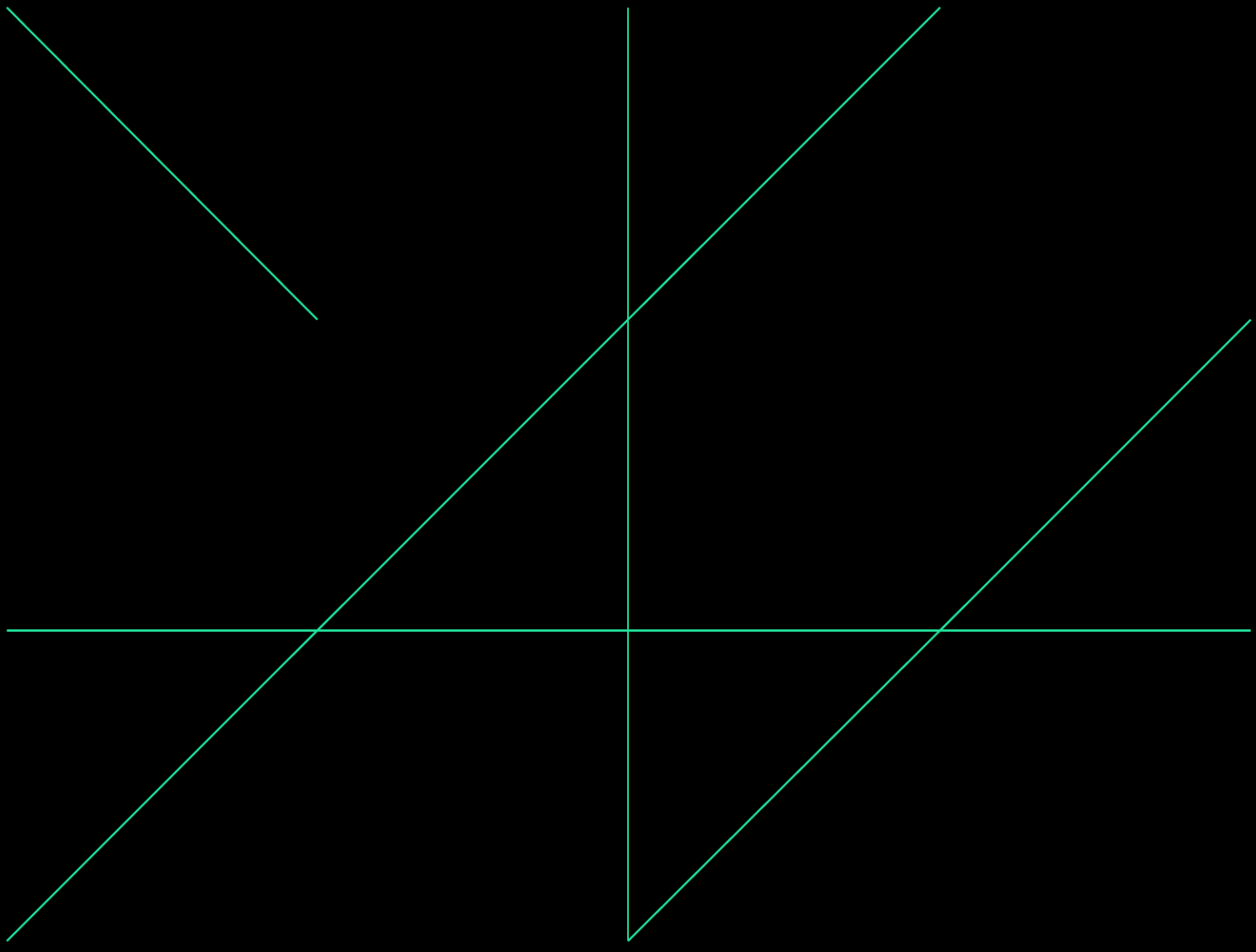
Mesure	Ce que demande le ReCyF	La réponse Seclab
7.A.7 EI · EE	Seules les interconnexions strictement nécessaires aux activités ou au MCO/MCS sont mises en œuvre, entre l'ensemble des SI concernés et le reste	**Xplore - Xchange** Cœur d'offre Application matérielle du principe (Xchange) + détection continue des flux hors matrice (Xplore).
7.A.8 EE	Seules les interconnexions strictement nécessaires aux activités ou au MCO/MCS sont mises en œuvre, entre chaque SI	**Xplore - Xchange** Cœur d'offre Application matérielle du principe (Xchange) + détection continue des flux hors matrice (Xplore).
7.B.1 EI · EE	Définir et documenter les communications nécessaires	**Xplore** Cœur d'offre Matrice de flux observés, exportable. Le livrable peut être directement intégré au dossier de conformité.
7.B.2 EE	Définir et documenter les communications nécessaires, y compris entre sous-systèmes.	**Xplore** Cœur d'offre Matrice de flux observés, exportable. Le livrable peut être directement intégré au dossier de conformité.
7.B.3 **7.B.4** EI · EE	Règles de filtrage aux interconnexions, blocage par défaut, pare-feu(x) dédié(s) vers les SI tiers.	**Xchange** Cœur d'offre Deny-all matériel. Peut aussi être utilisé en double barrière d'un firewall.
7.B.5 EI · EE	Revue annuelle de la mise en œuvre technique des règles de filtrage.	**Xplore** Contribution Identification des écarts entre la segmentation théorique et celle observée en continu. La preuve de revue peut ainsi être fournie.
8 Sécurisation des accès distants aux SI		
8.1 EI · EE	Protéger les accès effectués via un SI tiers (chiffrement conforme aux recommandations ANSSI).	**Xplore - Xchange** Contribution Xplore permet d'identifier les accès distants directs (qui ne passeraient pas par le bastion). Xchange apporte la rupture protocolaire matérielle sur les flux de télémaintenance, en complément du bastion / VPN.
9 Protection des SI contre les codes malveillants		
9.3 **9.2** **9.4** EI · EE	Seuls les matériels gérés par l'entité se connectent ; empêcher la connexion des autres.	**Xplore** Contribution Détection immédiate de tout nouvel équipement connecté au réseau OT. Mesure de contrôle de la politique matérielle.
9.5 EI · EE	Seuls les supports amovibles nécessaires se connectent aux SI.	**Xport** Cœur d'offre Point de passage obligé pour les médias amovibles. Xport matérialise et fait respecter la politique.
9.6 EI · EE	Mécanismes de protection contre l'exécution de codes malveillants sur les ressources traitant des données externes.	**Xport** Contribution Compense l'impossibilité d'installer antivirus / EDR sur les équipements OT anciens ou propriétaires. Isolation des ports USB et filtrage des fichiers qui n'ont pas été inspectés par une station blanche
9.7 EI · EE	Analyse des données de sources externes à réception. Exemple cité : « SAS de décontamination antivirale pour les clefs USB ».	**Xport** Contribution Xport s'assure que seuls les fichiers passés par l'analyse de données pourront accéder aux systèmes cibles.
11 Maîtrise de l'administration des SI		
11.B.5 EE	Interdire par un dispositif de filtrage les connexions externes vers les ressources d'administration du cœur de confiance.	**Xchange** Contribution Dispositif de filtrage matériel positionné devant les ressources d'administration du cœur de confiance (annuaires).

Toutes les mesures couvertes (suite)

Mesure	Ce que demande le ReCyF	La réponse Seclab
12 Identification et réaction aux incidents de sécurité		
12.3 EI · EE	Mécanismes d'analyse et de qualification des événements, identification des incidents potentiels ou avérés.	**Xplore** Cœur d'offre 4 moteurs de détection (cartographie, règles Sigma, signatures Suricata, comportemental IA), alertes contextualisées, capacités d'analyse forensique, archivage des paquets
12.4 EE	Mécanismes organisationnels et techniques permettant de réagir en cas d'incident	**Xplore** Contribution Identification du responsable opérationnel des actifs et des process concernés
12.7 EE	Relevés techniques protégés d'un incident qui les rendrait inexploitables (ex. rançongiciel).	**Xplore - Xchange** Contribution Export unidirectionnel des relevés vers une zone isolée, hors d'atteinte d'un attaquant. Xplore assure la collecte et l'archivage sécurisé des paquets (preuves en cas d'incident).
13 Continuité et reprise d'activité		
13.3 EI · EE	Sauvegardes protégées d'un incident les rendant inexploitables (ex. rançongiciel, stockage hors ligne).	**Xchange** Cœur d'offre Isolation matérielle du réseau et des dépôts de sauvegarde. Xchange assure notamment ce type de protection pour les dépôts de sauvegarde de DELL.
14 Réaction aux crises d'origine cyber		
14.8 EE	Mise en œuvre de mesures pour isoler, protéger et reconstruire	**Xport** Contribution Xport permet de basculer en mode isolation complète (déconnexion réseau totale) avec utilisation sécurisée de media amovibles
17 Audit de la sécurité des systèmes d'information		
17.3 EE	L'audit de sécurité comprend un audit d'architecture	**Xplore** Contribution Xplore fournit une vision réelle de l'architecture OT
18 Sécurisation de la configuration des ressources		
18.4 EE	Revue annuelle de configuration des ressources, outillage automatisé recommandé.	**Xplore** Contribution Observation passive des vulnérabilités et des écarts, des configurations des pare-feux. Xplore alimente et outille la revue annuelle.
19 Administration depuis des ressources dédiées		
19.8 EE	Cloisonnement et filtrage du réseau d'administration ; cloisonnement des flux d'administration transitant sur des réseaux non dédiés.	**Xchange** Cœur d'offre Ségrégation physique du réseau d'administration vis-à-vis des réseaux de production.
19.9 EE	Mesures de réduction du risque quand la liaison physique dédiée est impossible.	**Xchange** Contribution Mesure de réduction du risque « prête à l'emploi » avec isolation matérielle sur le chemin d'administration.
20 Supervision de la sécurité des systèmes d'information		
20.1 **20.2** EE	Capacité opérationnelle de traitement des événements sous 24 h ; démarche d'amélioration continue de la supervision.	**Xplore** Contribution Réduction du bruit et des faux positifs, alertes qualifies. Xplore rend la capacité 24 h soutenable ; élargissement progressif des sources et scénarios.
20.3 **20.4** EE	Maîtrise du SI de supervision ; collecte de journaux et événements reflétant la variété des activités (réseau, système, applicatif).	**Xplore** Cœur d'offre Sondes passives OT alimentant le SOC / SIEM existant (interopérabilité native), sans impacter le procédé.
20.5 **20.6** EE	Conservation des journaux au moins 3 mois ; protection contre un incident les rendant inexploitables.	**Xchange** Contribution Remontée unidirectionnelle OT → IT des journaux sans exposer l'OT ; copie conservée hors d'atteinte.

seclab®

Next-Gen OT
Cybersecurity Platform



205 impasse John Locke
34470 Pérols, France.

seclab-security.com