
seclab.®

L’OT est en danger

Mais plus pour longtemps

Les infrastructures numériques critiques et industrielles sont en danger.

Les solutions IT ne fonctionnent pas pour l'OT !

Les industriels n'ont pas d'autres choix que de s'équiper de technologies Américaines, Israéliennes ou Asiatiques.

Mais plus pour longtemps...

Vos opérations tournent. Quid de leurs défenses ? ®

Une convergence IT/OT bien avancée

70%

Des systémes OT sont connectés aux réseaux IT en 2025 (1)

+44%

De dispositifs OT exposés sur Internet sur une année (2)

Une cible devenue privilégiée

22%

Des entreprises OT ont subi un incident cyber en 2024 (3)

40%

De ces incidents ont généré un arrêt d'activité (3)

Nécessaire montée en maturité cyber

86%

Des sociétés OT ne sont pas préparées face aux menaces (3)

69%

Des entreprises OT n'ont pas d'inventaire à jour (4)

Les limites des solutions actuelles

53%

Des alertes de sécurité sont des faux positifs (5)

2 à 10

Correctifs de sécurité à appliquer par mois sur un firewall OT(6)

Les contraintes réglementaires

Les réglementations s'appliquent de plus en plus à l'OT

- **NIS2**
- **Directive CER**
- **Cybersecurity Act**
- **IEC62443**

(1) Telstra/Omdia – 2025
(2) SOCRadar – 2025
(3) SANS Institute - 2025
(4) Ponemon - 2024
(5) SentinelOne - 2025
(6) Etude Seclab basée sur l'analyse de 5 éditeurs

seclab.

Seclab, Confiance + Innovation ®

Confiance

50
Collaborateurs

1/3
Des déploiements à l'international

100%
De capitaux européens

VISA DE SÉCURITÉ — ANSSI
Certification CSPN

Innovation

NREL
Certifié best product for network segregation

Gartner
COOL VENDOR

6
Brevets

Naval Partners Meeting 2025 — NAVAL GROUP
Operational Excellence Award Naval Group

Hardware | Logiciel embarqué | IA

Recommandé par les experts ®

McKinsey & Company

”With their robust and certified products they discovered a niche at the interface of the IT and OT worlds. „

BCG

”A unique technology with an Europeen DNA, powered by a teams of security professionals who understand the security needs of the world’s most critical OT networks, differentiates SecLab from its competitors. „

Gartner

”Besides blocking network cyberattacks, who may have penetrated your IT network and are carrying out reconnaissance will never be able to see any information about your OT network. „

Wam Voster, Cool Vendors in Cyber-Physical Systems Security

+ Nommé dans les Hype Cycle 2025 CPS Security et Zero-Trust Technology

seclab.

Reconnu par de grands noms de l'OT ®

Industrie, Production

sanofi

ARKEMA

SIEMENS

SAINT-GOBAIN

BOUYGUES CONSTRUCTION

CLARINS PARIS

Givaudan

Menissez — french baker since 1965

Transport, Logistique, Services

SNCF RÉSEAU

ALSTOM

tepsa

suez

sourcéo

AQSACOM Innovating Intelligence

bouygues TELECOM

orange™

Energie

EDF

framatome

TotalEnergies

NATIONAL GRID CORPORATION OF THE PHILIPPINES · NGCP

دانة غاز DANA GAS

PG&E

cea

TERĒGA

Westinghouse

Public, Recherche

MINISTÈRE DE LA JUSTICE
Liberté Égalité Fraternité

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

Région îledeFrance

BỘ KẾ HOẠCH VÀ ĐẦU TƯ · MINISTRY OF PLANNING AND INVESTMENT

cnrs

métropole GrandNancy

SAINT BRIEUC ARMOR AGGLOMÉRATION

Aero, Défense, Espace

MINISTÈRE DES ARMÉES
Liberté Égalité Fraternité

THALES

AIRBUS

arianeGROUP

cnes

NAVAL GROUP

nexter

seclab.

Sélectionné par des partenaires exigeants ®

OT Cybersecurity Platform de Seclab ®

La seule CPS Protection Platform* qui combine Visibilité de l'infrastructure OT, Détection des menaces et Protection des actifs sensibles, pour une défense en profondeur.

La seule CPS Protection Platform* Européenne.

* Dénomination employée par Gartner pour désigner les plateformes de cybersécurité des environnements OT.
CPS = Cyber-Physical Systems

OT Cybersecurity Platform de Seclab ®

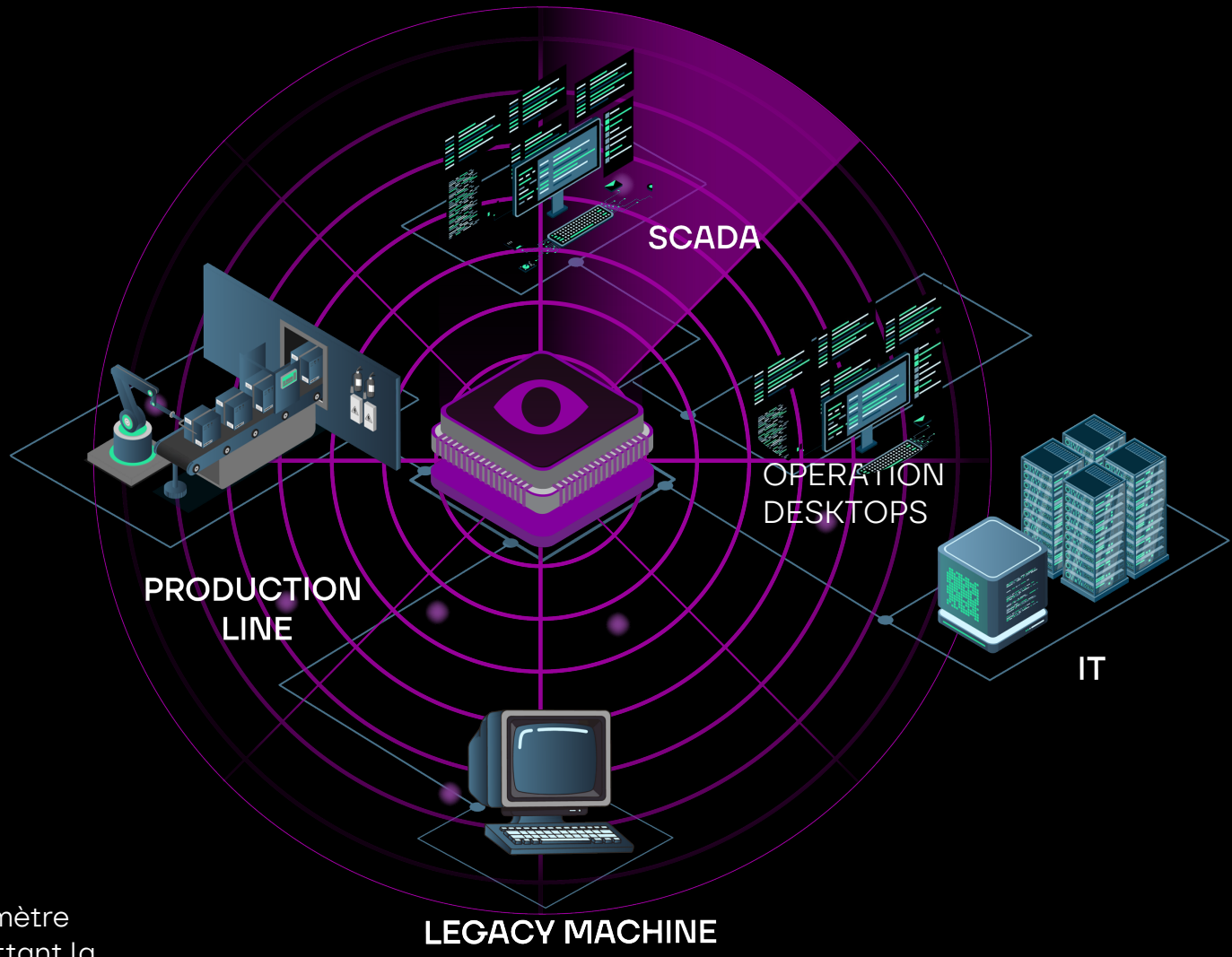
DISCOVER

ISOLATE

DETECT

Développer la connaissance de l'environnement OT

- Découverte des actifs et flux
- Inventaire et cartographie
- Détection des vulnérabilités
- Définition des actifs critiques et des flux à autoriser (**MVDI**)



MVDI = Minimum Viable Digital Industry | Périmètre contenant uniquement les actifs vitaux permettant la continuité de fonctionnement de l'entreprise

OT Cybersecurity Platform de Seclab ®

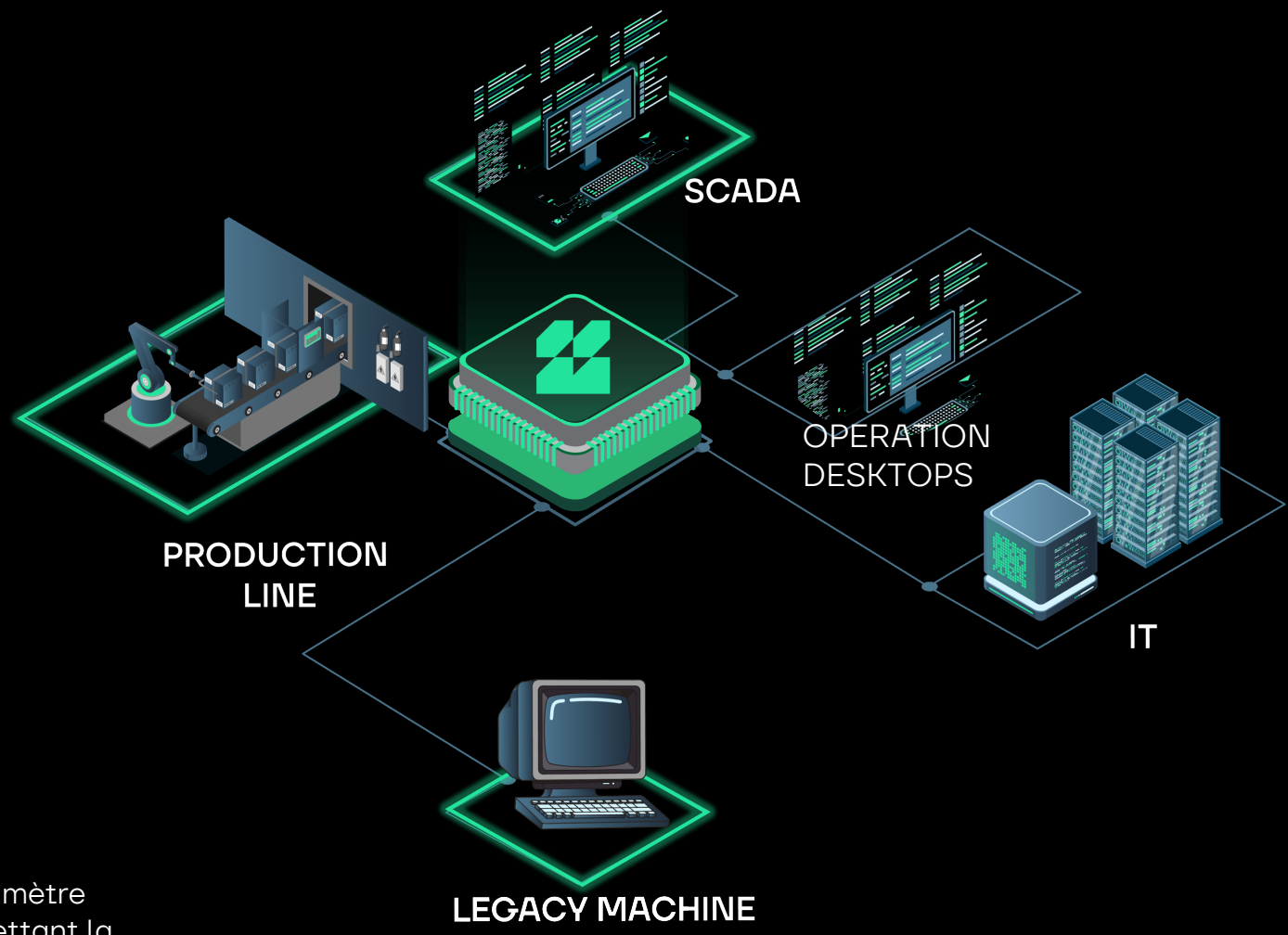
DISCOVER

ISOLATE

DETECT

Mettre en place une protection efficace basée sur la découverte

- Protection des actifs critiques (**MVDI**) par isolation physique réseau et USB (legacy ou équipements non connectés) grâce à l'Electronic AirGap™



MVDI = Minimum Viable Digital Industry | Périmètre contenant uniquement les actifs vitaux permettant la continuité de fonctionnement de l'entreprise

OT Cybersecurity Platform de Seclab ®

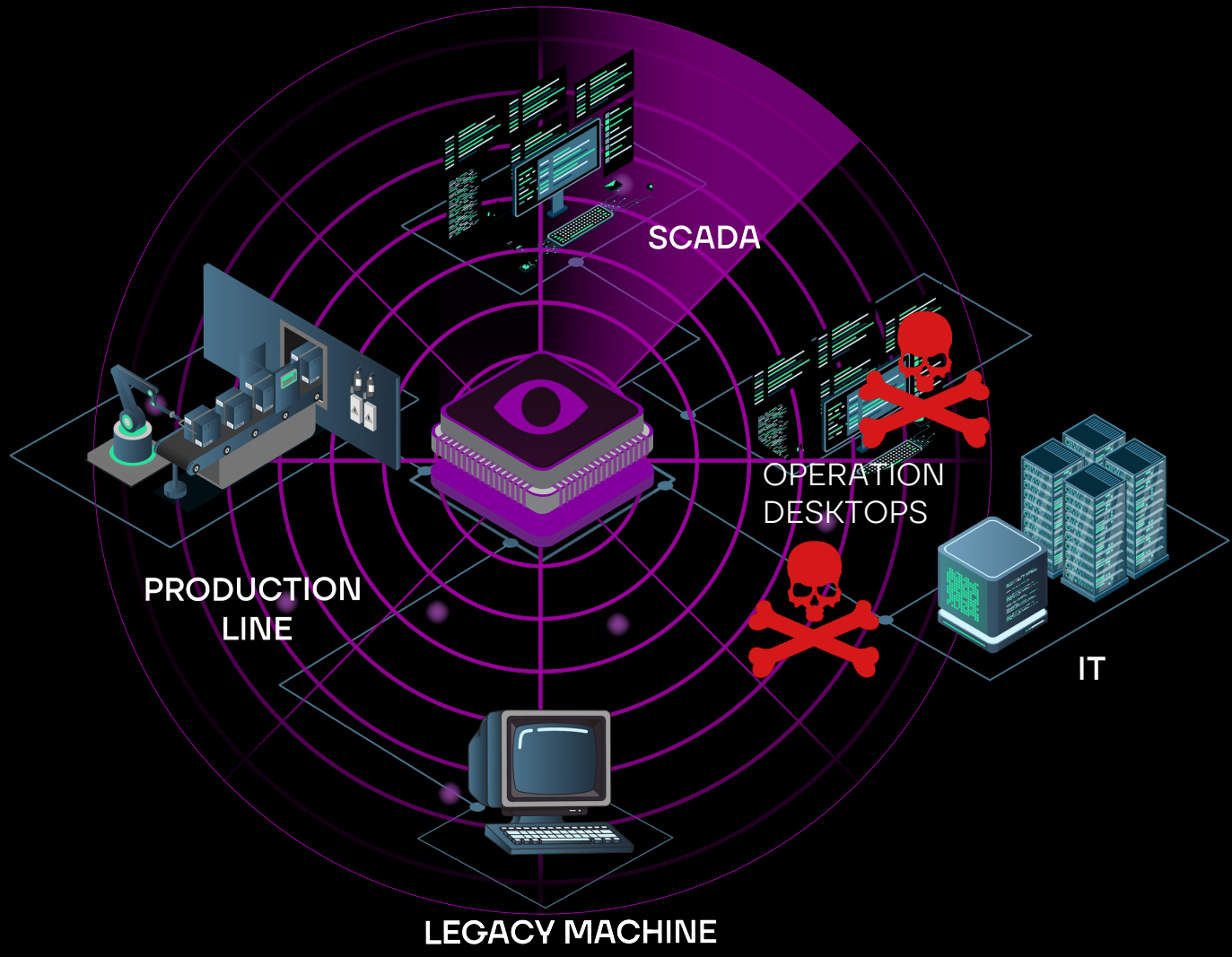
DISCOVER

ISOLATE

DETECT

Surveiller en continue les menaces et les anomalies

- Réduction du périmètre de surveillance grâce à l'isolation
- Identification des écarts (nouveaux flux, actifs, comportements)
- Détection temps réel des menaces et anomalies, boostée par l'IA



Une démarche progressive pour sécuriser l'OT ®

DISCOVER

Développer la connaissance de l'environnement OT

0	Identifier tous ses actifs et ses flux OT
1	Réaliser un inventaire des actifs, une matrice des flux et une cartographie réseau
2	Identifier les vulnérabilités
3	Définir les actifs critiques à protéger (MVDI) et les flux métier à autoriser

ISOLATE

Mettre en place une protection efficace basée sur la découverte

4	Isoler le périmètre MVDI au niveau réseau
4	Isoler le périmètre MVDI au niveau USB, pour les actifs non connectés ou legacy
5	Hors MVDI, réaliser une segmentation avec des équipements de sécurité standards

DETECT

Surveiller en continu les menaces et les anomalies

6	Maintenir une surveillance continue des écarts (nouveaux actifs, flux, comportements)
7	Détecter les menaces et anomalies
8	Adapter l'isolation ou la segmentation si nécessaire

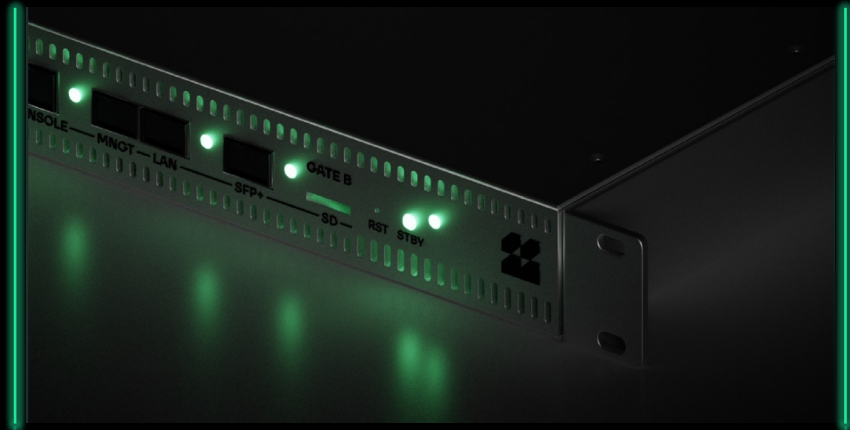
Seclab OT Maturity Response Model

MVDI = Minimum Viable Digital Industry | Périmètre contenant uniquement les actifs vitaux nécessaires à la continuité de fonctionnement de l'entreprise

3 produits pour une défense en profondeur ®

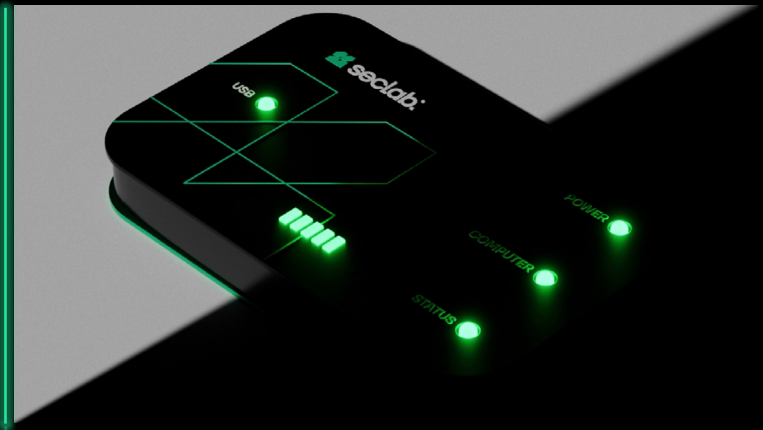
Xplore
See-First Intelligence

- Découverte OT non-intrusive
- Cartographie OT la plus complète du marché
- Vues multiples (Logique, Geographique, Purdue, Réseau/IT)
- Mode audit ou supervision
- Détection des menaces et anomalies augmentée par l'IA



Xchange Network
Set-and-Forget Security

- Isolation réseau sécurisée avec l'Electronic AirGap breveté
- Flux bidirectionnels à faible latence
- Filtrage des fichiers et applications
- Immunisé face aux O-day
- Pas d'effort de mises à jour
- Administration Zero-Trust



Xchange USB
Plug-and-Protect Technology

- Isolation USB sécurisée avec l'Electronic AirGap breveté
- Protection USB à toute épreuve
- Filtrage de fichiers, contrôle d'intégrité
- Assure la continuité opérationnelle
- Aucune installation logicielle requise
- Non intrusif pour les systèmes Legacy

seclab.

Une cybersécurité conçue pour l'OT ®

Démarche méthodologique supportée par la plateforme

= *montée en maturité progressive*

Cartographie intégrant des vues OT et IT

= *meilleure collaboration*

Segmentation par isolation physique

= *sécurité immuable*

Sécurité non-intrusive et sans effort de maintenance

= *faibles impacts opérationnels*

Détection des écarts et des anomalies

= *moins de charge d'analyse*

Conformité réglementaire par conception

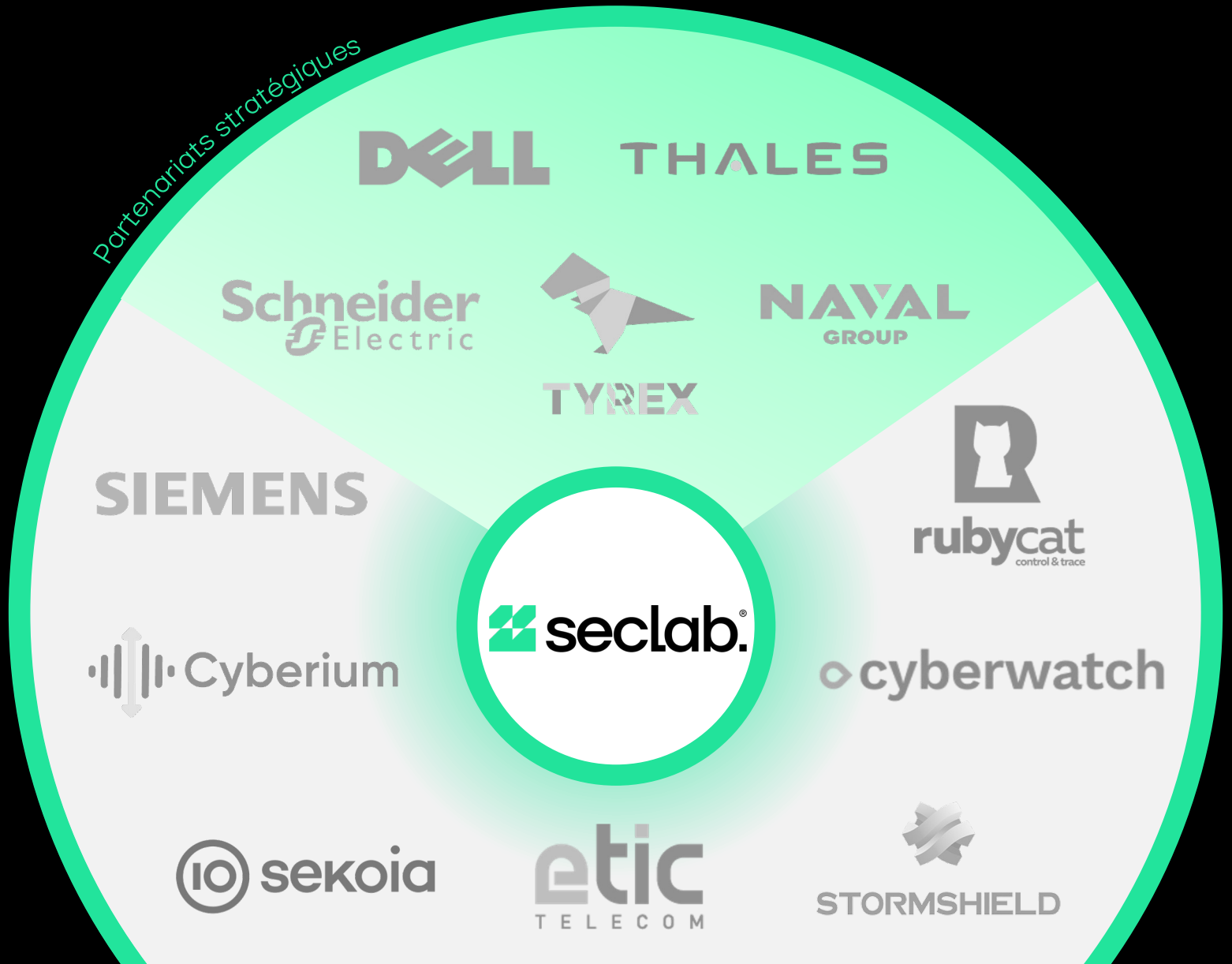
= *tranquilité d'esprit*

Des dépendances maîtrisées ®

Sur toute la chaîne de développement et d'approvisionnement

ITAR Free
Cloud Act Free

Un écosystème complémentaire ®



seclab®

Cas d’usages.

Cas d'usage Pharmaceutique ®

✳ **Challenge :**

Sécurisation des flux IT/OT pour une production conforme, continue et résiliente.

✳ **Besoins :**

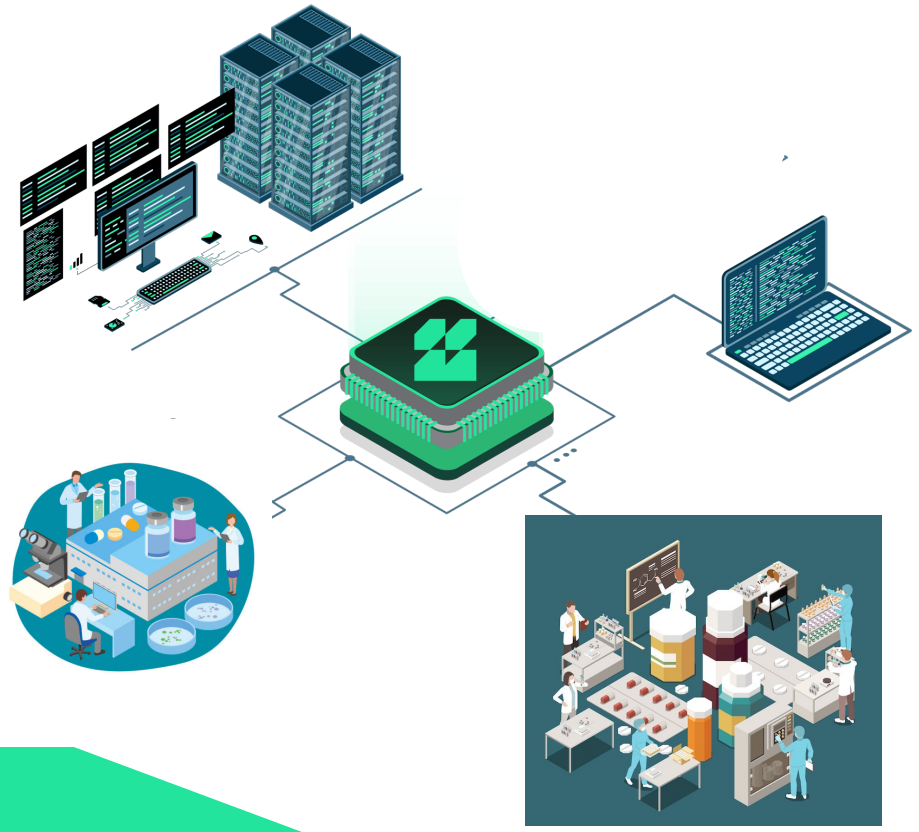
- **Échanger les données de production avec le système informatique (contrôle qualité, R&D,…) sans exposer les systèmes industriels**
- Éviter tout compromis des automates, interfaces utilisateur et équipements critiques
- Rassurer les équipes qualité et conformité concernant la sécurité des échanges

✳ **Démarche :**

- Comparaison de plusieurs technologies (fw, diode, rupture protocolaire/hardware)

✳ **Solution retenue :**

Seclab (rupture protocolaire hardware)

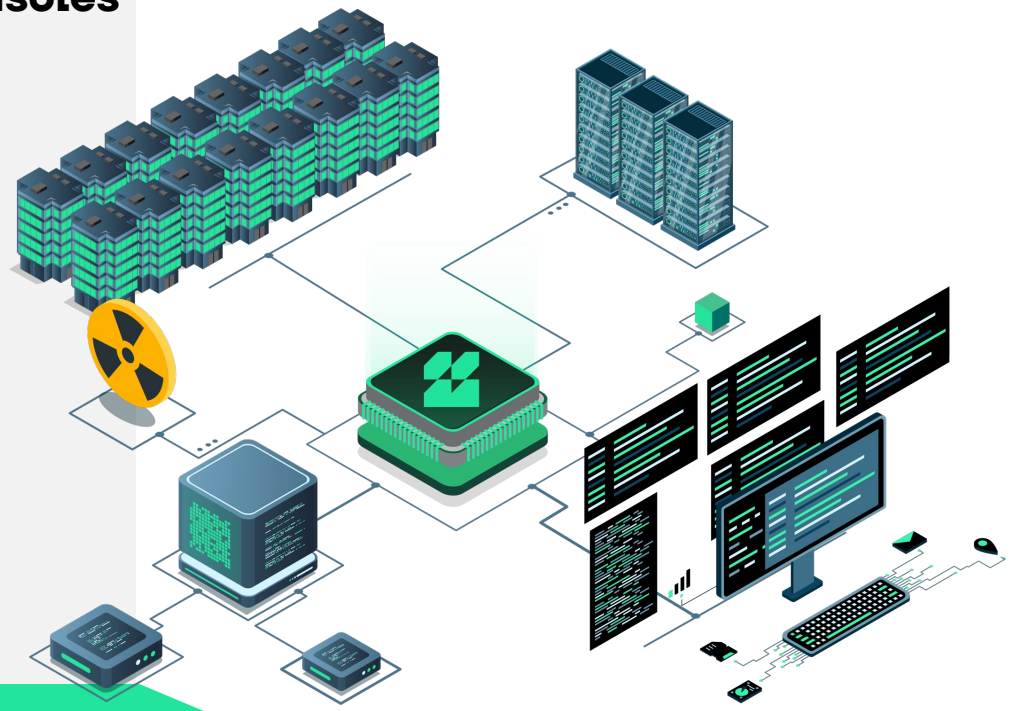


Bénéfices clients :

- **Isolation physqiue :** segmentation et ségrégation réseau à 100 %
- **Conformité réglementaire :** Architecture certifiée CSPN par l'ANSSI
- **Résistant au zero-day :** Protection contre les attaques sur les couches réseau et le système d'opération
- **Support long time**

Cas d'usage Recherche ®

- **Challenge :**
  Management centralisé d'un SOC avec des environnements isolés
- **Besoins :**
  - Collecte de logs sécurisés
  - Synchronisation du temps entre les différents SI
  - +de 30 SI isolés
- **Démarche :**
  - Comparatif entre plusieurs types de technologie (diode, rupture hardware)
  - Validation du niveau d'isolation
  - Test de la collecte des logs des sondes NDR et synchronisation NTP
- **Solution retenue :**
  Seclab (rupture protocolaire hardware)

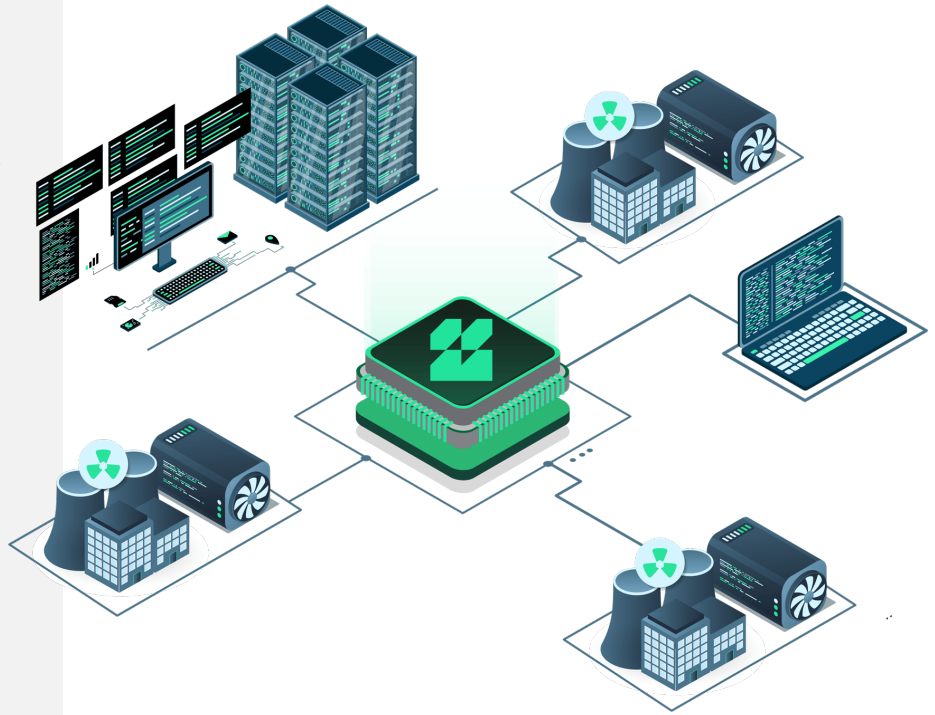


Bénéfices client :

- **Isolation physique bidirectionnelle** : SXN isole et masque physiquement les 3 environnements
- **Conformité règlementaire** : Architecture certifiée conforme par l'ANSSI
- **Simplification de l'administration** vs une architecture avec diode
- **Principe de gouvernance :** séparation des responsabilités avec les ½ règles

Cas d'usage Nucléaire ®

- **Challenge : Digitalisation des usages**
- **Besoins :**
  - Protéger la sécurité et la fiabilité des systèmes critiques tout en permettant la configuration du système et les mises à jour logicielles.
  - Pérenniser l'usage de systèmes qu'on ne peut plus mettre à jour.
  - Permettre l'échange de données entre des réseaux de gouvernances différentes.
  - **Isolation d'un centre de contrôle d'une centrale nucléaire avec l'IT**
- **Démarche :**
  - Comparatif entre plusieurs types de technologie (fw, diode, rupture protocolaire applicative/matérielle)
- **Solution retenue :**
  Seclab (rupture protocolaire hardware)



Bénéfices client :

- **Isolation physique :** segmentation et ségrégation du réseau à 100 %.
- **Conformité règlementaire :** Produit certifié CSPN par l'ANSSI.
- **Insensible au zero-day :** Protège des attaques sur les couches réseau et système d'exploitation.
- **Long time support**

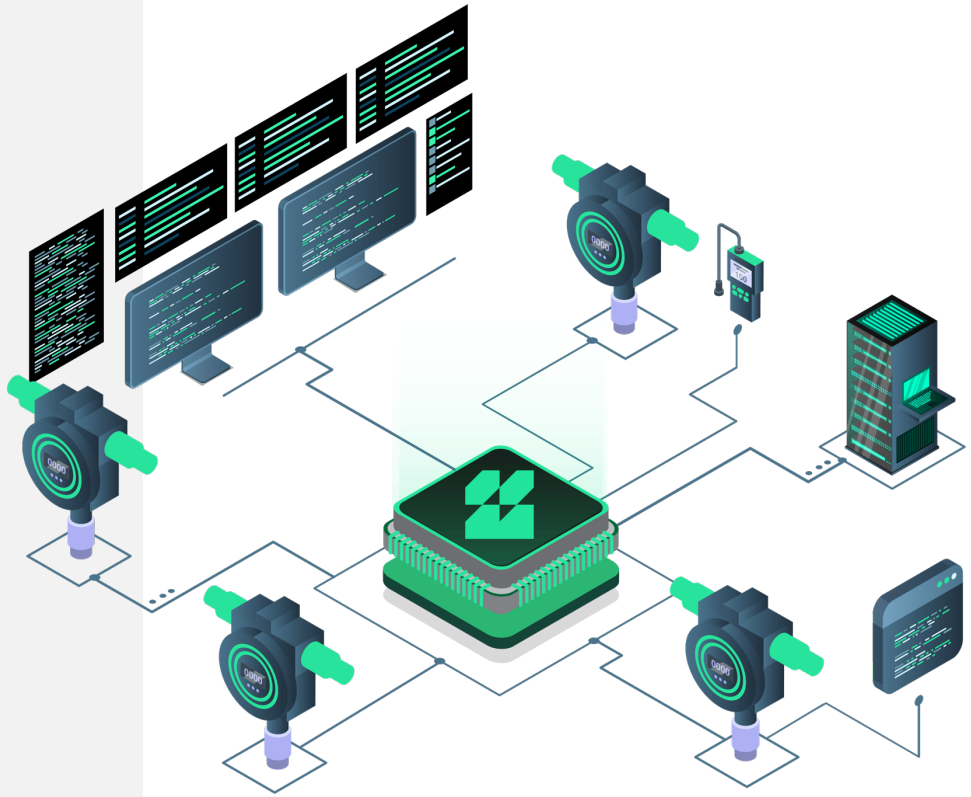
Cas d'usage Energie ®

✳ **Challenge :**
Digitalisation des usages

✳ **Besoins :**
- Interconnexion IT / OT
- Isolation de l'interconnexion avec des tiers
- Sans temps de latence
- **Échanges bi-directionnels entre les capteurs et la salle de contrôle**

✳ **Démarche :**
- Comparatif entre plusieurs types de technologie (diode, rupture hardware)
- Validation du niveau d'isolation
- Temps de latence < 1ms

✳ **Solution retenue :**
Seclab (rupture protocolaire hardware)



Bénéfices client :
- **Isolation physique bidirectionnelle :** SXN isole et masque physiquement les 2 environnements
- **Conformité règlementaire** : Architecture certifiée au niveau cyber et au niveau sureté
- **Simplification de l'administration** vs une architecture avec diode
- **Principe de gouvernance :** séparation des responsabilités avec les ½ règles

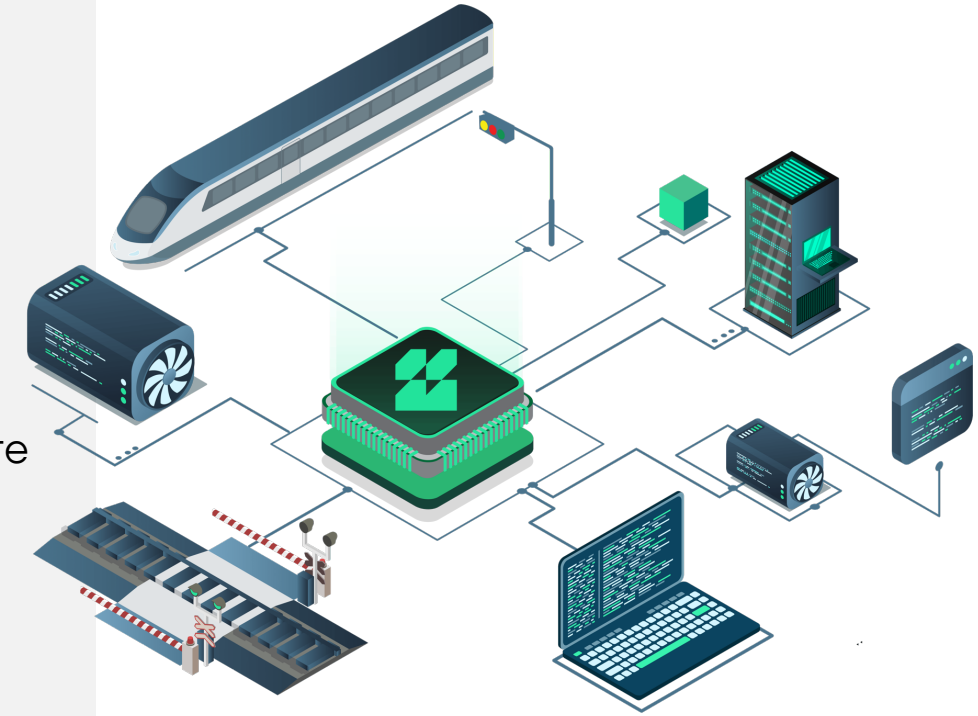
Cas d'usage Transport ®

✳ **Challenge :**
Digitalisation des usages & ouverture à la concurrence

✳ **Besoins :**
- Interconnexion IT / OT
- Mise en conformité réglementaire
- Isolation de l'interconnexion avec des tiers
- **Isolation entre le réseau de signalisation et le réseau IT**

✳ **Démarche :**
- Comparatif entre plusieurs types de technologie (fw, diode, rupture protocolaire applicative/matérielle)
- Validation du niveau de sécurité avec la valise OTAN
- Validation fonctionnelle de l'architecture (flux applicatifs)

✳ **Solution retenue :**
Seclab (rupture protocolaire hardware) + Stormshield (analyse applicative)



Bénéfices client :
- **Isolation physique :** SXN isole et masque physiquement les 2 environnements
- **Conformité règlementaire ZEHO :** Architecture certifiée conforme par l'ANSSI
- **Insensible au zero-day :** Pas de dépendance au correctif logiciel
- **Long time support**

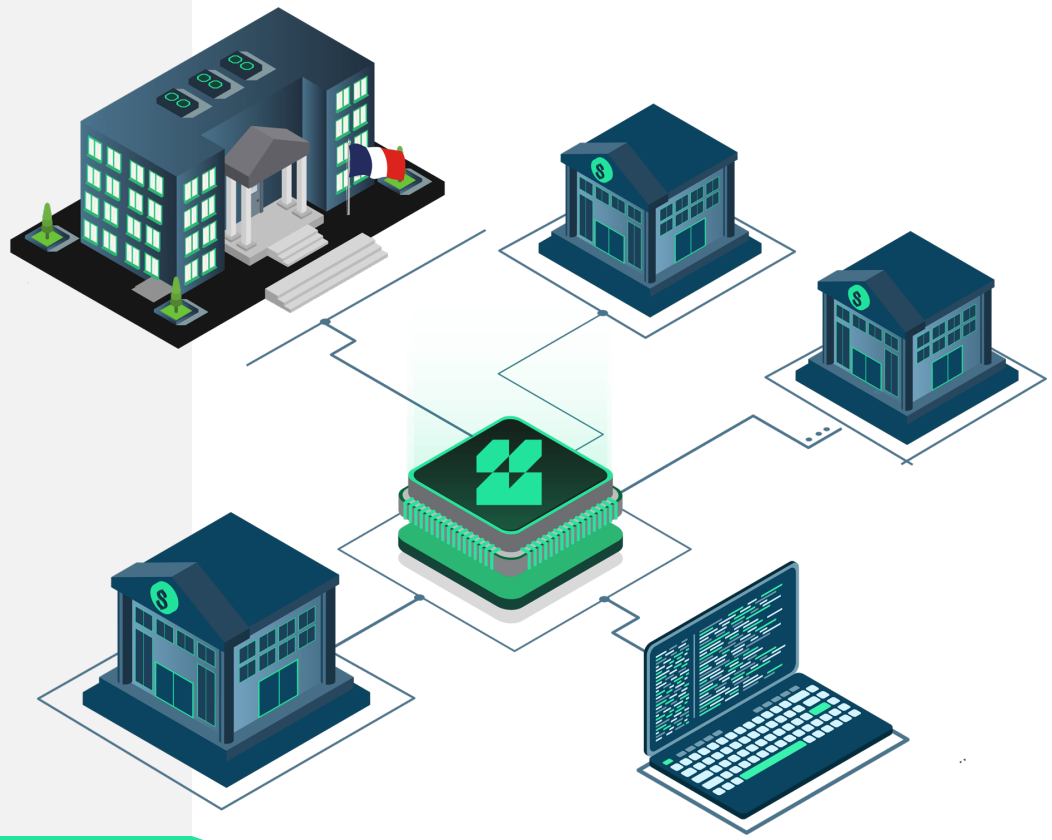
Cas d'usage Ministère public ®

✳ **Challenge :**
Ouverture maîtrisée du SI avec des tiers & Isolation de l'application vis-à-vis du réseau interne

✳ **Besoins :**
- Ouverture et isolation d'une application critique
- DLP physique
- Plateforme d'échange de fichiers XML
- Sécurisation des communications TCP/IP avec des tiers

✳ **Démarche :**
- Comparatif entre plusieurs types de technologie (fw, diode, rupture hardware)
- Validation du niveau de sécurité
- Validation fonctionnelle du DLP physique

✳ **Solution retenue :**
Seclab (rupture protocolaire hardware)



Bénéfices client :
- **Isolation physique bidirectionnelle :** SXN isole et masque physiquement les 3 environnements
- **Insensible au zero-day :** Pas de dépendance au correctif logiciel
- **Optimisation des coûts :** Solution agnostique sur les protocoles traversants

seclab®

The Cyber-physical systems company

MERCI

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