
seclab.®

OT is no longer a sanctuary

The explosion of connections and the growing sophistication of threats have made industrial systems a prime target.

OT is under imminent threat

For industrial and sensitive organizations
seeking to maintain control over their critical and OT perimeters,
Seclab is the ally that multiplies their superpowers.

Strengthen your command of this new battlefield

Critical digital and industrial infrastructures are under threat.

IT solutions don't work for OT!

Industrial companies have no choice but to rely on American, Israeli, or Asian technologies.

We are here to change this paradigm

Your operations run. What about their defenses? ®

Skyrocketing OT connectivity

70%

Of OT systems are connected to IT networks by 2025(1)

+44%

Of OT devices exposed on the Internet over a year(2)

OT is a prime target

22%

Of OT companies experienced a cyber incident in 2024(3)

40%

Of those incidents caused an operational shutdown(3)

Necessary rise in cyber maturity

86%

Of OT companies are unprepared against threats(3)

69%

Of OT companies do not have an up-to-date inventory(4)

Limits of current solutions

53%

Of security alerts are false positives (5)

2 to 10

Security patches to be applied monthly on an OT Firewall(6)

Regulatory constraints

Regulations are increasingly being applied to OT

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

(1) Telstra/Omdia – 2025
(2) SOCRadar – 2025
(3) SANS Institute - 2025
(4) Ponemon - 2024
(5) SentinelOne - 2025
(6) Seclab study based on the analysis of 5 vendors

seclab.

Seclab, Trust + Innovation ®

Trust

50
Employees

1/3
Of deployments are international

100%
French capital

VISA DE SÉCURITÉ — ANSSI
CSPN Certified

Innovation

NREL
Certified best product for network segregation

Gartner
COOL VENDOR

6
Patents

Naval Partners Meeting 2025 NAVAL GROUP
Operational Excellence Award Naval Group

Hardware | Embedded Software | AI

seclab.

Endorsed by 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 European DNA, powered by a team 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

+ Recognized in the Gartner Hype Cycle 2025 for CPS Security and Zero-Trust Technology

seclab.

Trusted by leading organizations in OT ®

Industry, Manufacturing

sanofi

ARKEMA

SIEMENS

SAINT-GOBAIN

BOUYGUES CONSTRUCTION

CLARINS PARIS

Givaudan

Menissez — french baker since 1965

Transport, Logistics, Services

SNCF RÉSEAU

ALSTOM

tepsa

AQSACOM Innovating Intelligence

suez

bouygues TELECOM

orange™

Energy

EDF

framatome

TotalEnergies

NATIONAL GRID CORPORATION OF THE PHILIPPINES · NGCP

دانة غاز DANA GAS

PG&E

cea

TERĒGA

Westinghouse

Public Sector, Research

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, Defence, Space

MINISTÈRE DES ARMÉES
Liberté Égalité Fraternité

THALES

AIRBUS

arianeGROUP

cnes

NAVAL GROUP

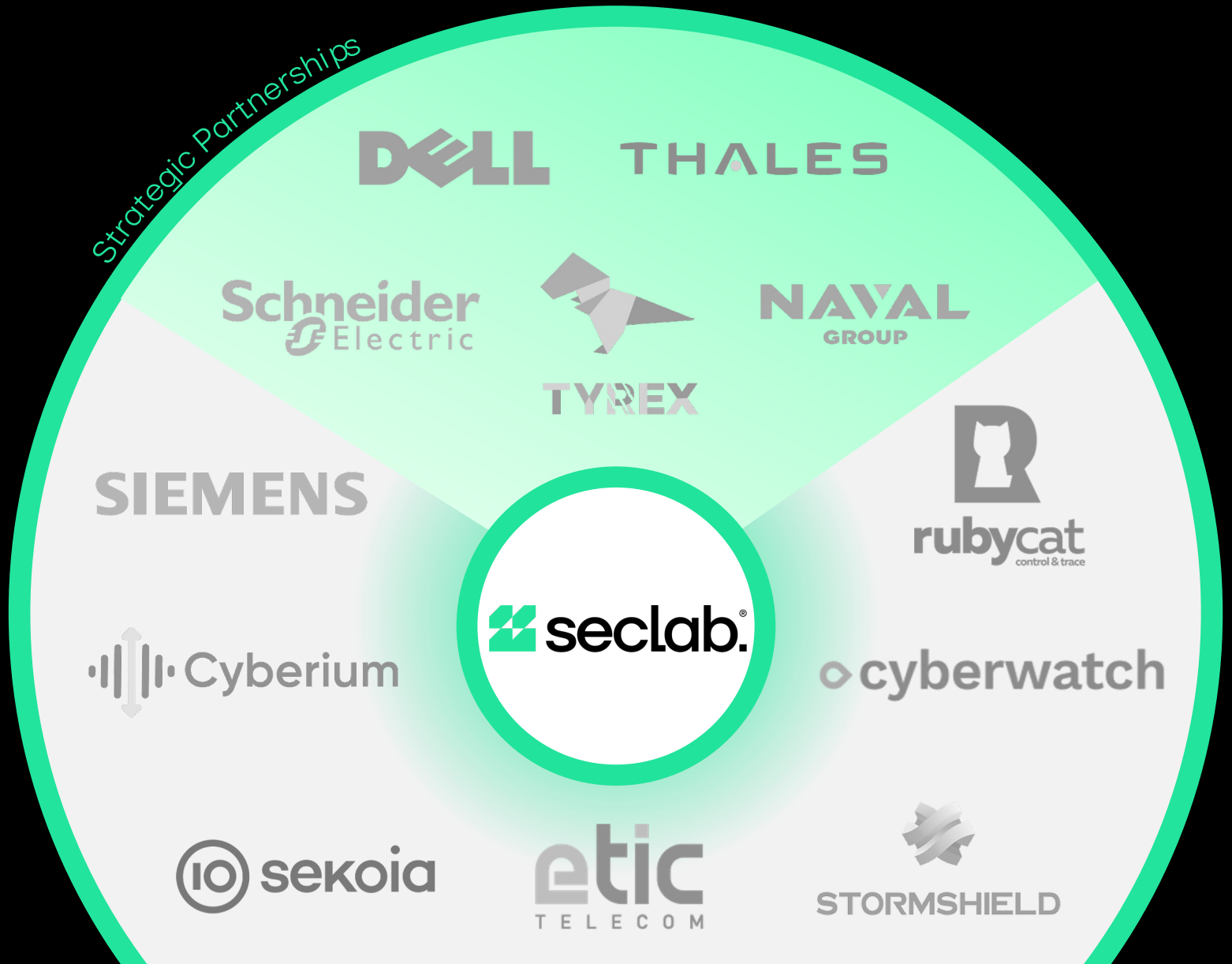
nexter

seclab.

Selected by demanding partners ®

seclab.

A powerful complementary ecosystem ®



Xcore

Seclab Xcore Platform

Next-Gen OT Cybersecurity Platform

The only OT Cybersecurity Platform that combines OT Infrastructure Visibility, Threat Detection and Critical Asset Protection — for true defense-in-depth.

The only European OT Cybersecurity Platform.

Seclab Xcore Platform ®

DISCOVER

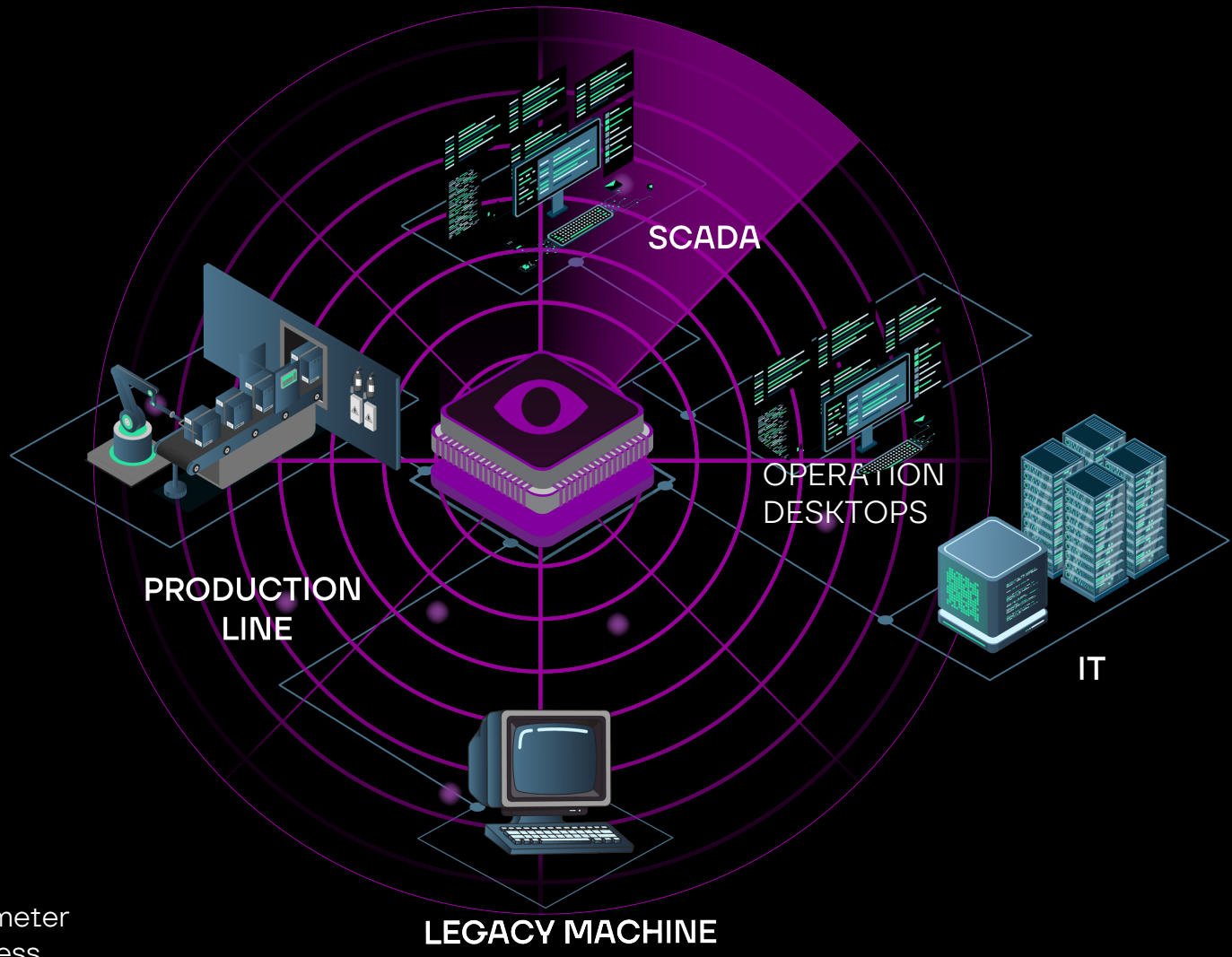
ISOLATE

DETECT

Building deep knowledge of the OT environment

- Asset and Data Flow Discovery
- Inventory and Mapping
- Vulnerability Detection
- Definition of Critical Assets and Authorized Flows (**MVDI**)

MVDI = Minimum Viable Digital Industry | Perimeter containing only the vital assets enabling business continuity



Seclab Xcore Platform ®

DISCOVER

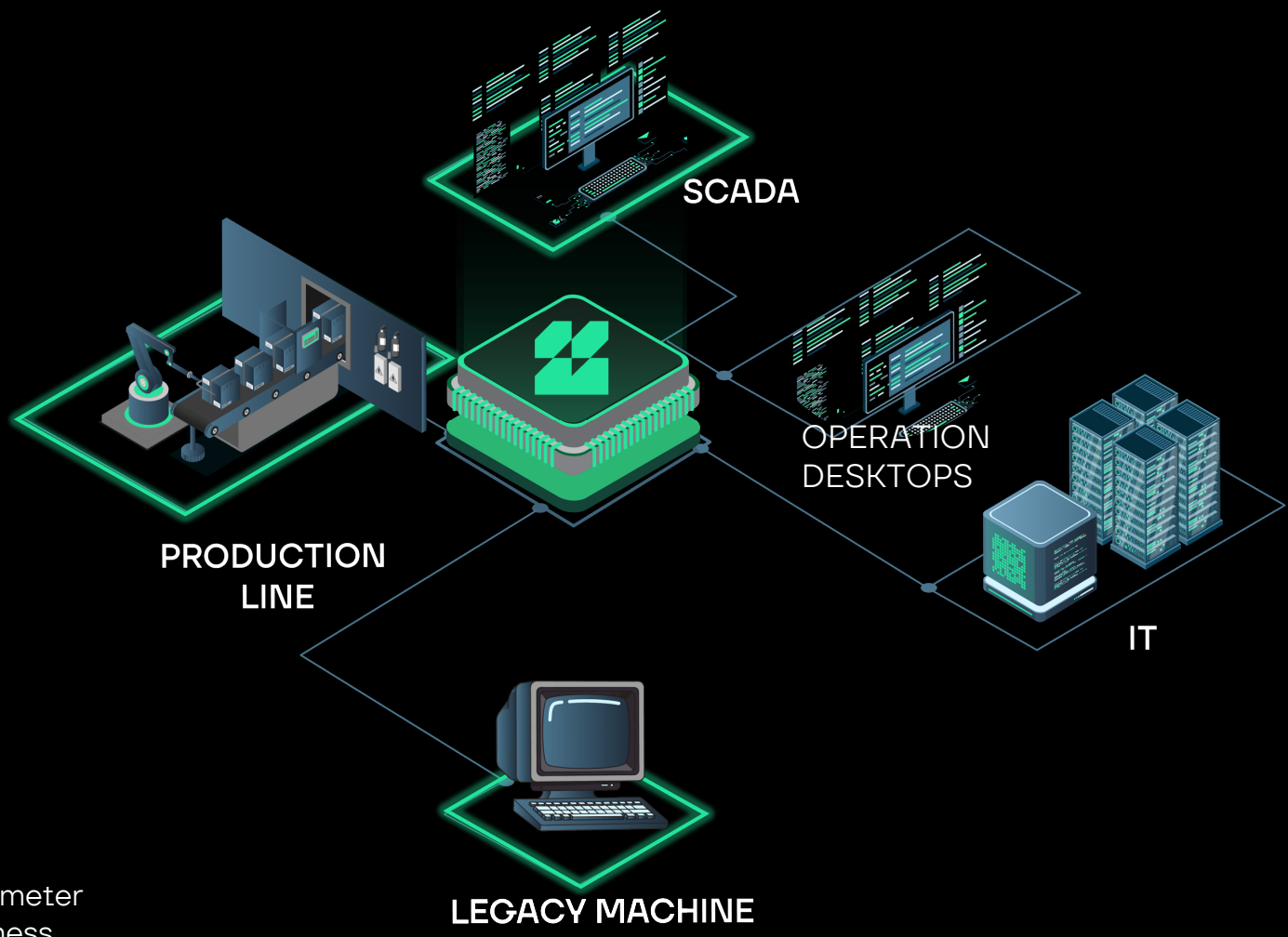
ISOLATE

DETECT

Deploying effective discovery-driven protection

- Protection of critical assets (**MVDI**) via physical network and USB isolation (legacy or non-connected equipment) through Electronic AirGap™

MVDI = Minimum Viable Digital Industry | Perimeter containing only the vital assets enabling business continuity



seclab.

Seclab Xcore Platform ®

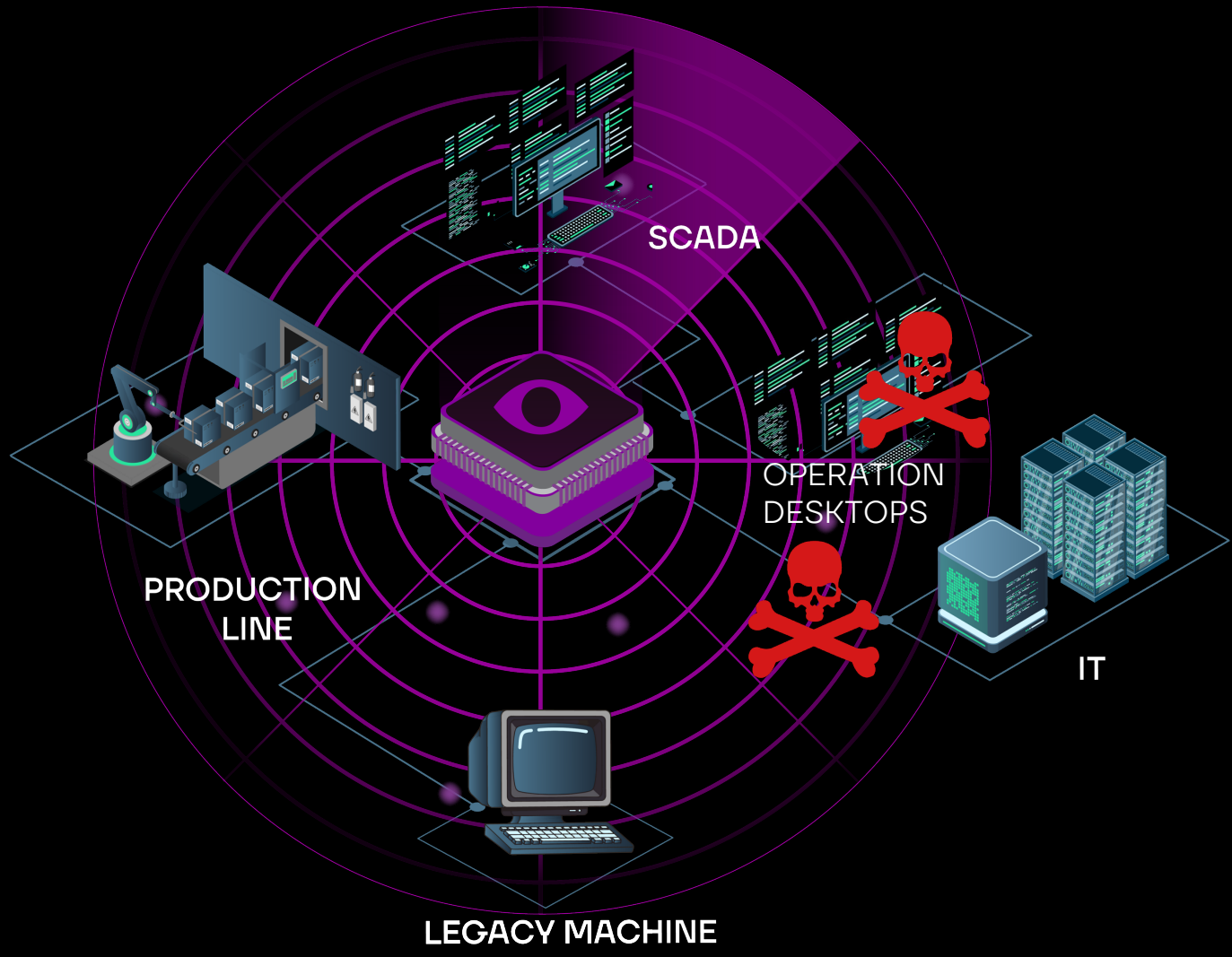
DISCOVER

ISOLATE

DETECT

Continuously monitoring threats and anomalies

- Reduced monitoring perimeter thanks to isolation
- Deviation identification (new flows, assets, behaviors)
- Real-time threat and anomaly detection, AI-powered



seclab.

A step-by-step approach to secure OT ®

DISCOVER

Building deep knowledge of the OT environment

0	Identify all your OT assets and flows
1	Build a comprehensive asset inventory, flow matrix, and network mapping
2	Pinpoint vulnerabilities
3	Define critical assets to protect (MVDI) and business flows to authorize

ISOLATE

Deploying effective discovery-driven protection

4	Isolate your MVDI perimeter at the network level
4	Secure the MVDI perimeter via USB isolation for non-connected or legacy assets
5	Beyond MVDI, implement segmentation using standard security appliances

DETECT

Continuously monitoring threats and anomalies

6	Maintain continuous monitoring of changes (new assets, flows, behaviors)
7	Detect threats and anomalies in real time
8	Adapt isolation or segmentation for mitigation

Seclab OT Maturity Response Model

MVDI = Minimum Viable Digital Industry | Perimeter containing only the vital assets required for business continuity

seclab.

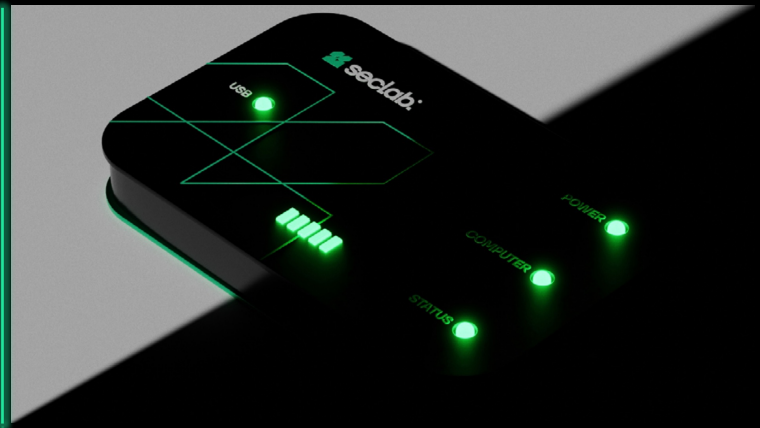
3 products for defense-in-depth ®

Xplore
See-First Intelligence

- Non-intrusive OT discovery
- Most comprehensive OT mapping on the market
- Multiple views (Logical, Geographic, Purdue, Network/IT)
- Audit or supervision mode
- AI-powered threat and anomaly detection

Xchange
Set-and-Forget Security

- Secure network isolation with patented Electronic AirGap
- Low-latency bidirectional flows
- File and application filtering
- Immune to zero-day attacks
- Zero patching effort
- Zero-Trust administration



Xport
Plug-and-Protect Technology

- Secure USB isolation with patented Electronic AirGap
- Bulletproof USB protection
- File filtering and integrity control
- Ensures operational continuity
- No software installation required
- Non-intrusive for legacy systems

seclab.

Cybersecurity built for OT ®

Platform-driven methodological approach

= *progressive maturity growth*

Unified mapping combining OT and IT views

= *better collaboration*

Segmentation through physical isolation

= *immutable security*

Non-intrusive security with zero maintenance overhead

= *minimal operational impact*

Deviation and anomaly detection

= *lower analysis overhead*

Compliance by design

= *peace of mind*

Full sovereignty, control of dependencies ®

Across the entire development and supply chain

ITAR Free
Cloud Act Free

use cases.

Pharmaceutical Use Case ®

⁎ Challenge :

Securing IT/OT flows for compliant, continuous, and resiliente production

⁎ Requirements :

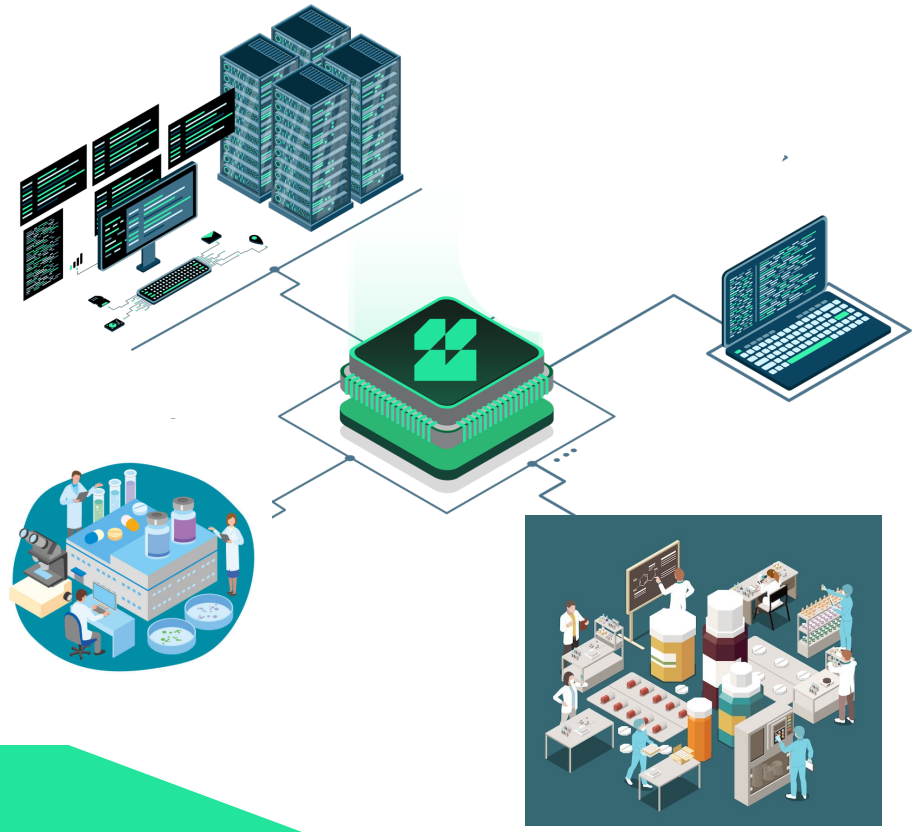
- **Exchange production data with the IT system (quality control, R&D,...) without exposing industrial systems**
- Avoid any compromise of automates, user interfaces and critical equipments
- Reassure the quality and compliance teams about the security of exchanges

⁎ Process :

- Comparison of several technologies (fw, diode, protocol break application/hardware)

⁎ Selected solution:

Seclab (hardware protocol break)



Customer benefits:

- **Physical isolation :** segmentation and segregation network at 100 %
- **Regulatory compliance :** Architecture certified CSPN by ANSSI
- (French Cybersecurity Agency)
- **Resistant to zero-day :** Attacks protection on network layers and operating system
- **Long time support**

Research Use Case ®

- **Challenge :**
  SOC centralized management with isolated environments
- **Requirements :**
  - Secured logs collection
  - Time synchronization between multiple IS
  - **SOC connected with 36 isolated SI**
- **Process :**
  - Comparison of several technologies (fw, diode, protocol break application/hardware)
  - Validation of isolation level
  - Collection test of logs from NDR probes and NTP synchronization
- **Selected solution :**
  Seclab (hardware protocol break)

Customer benefits :

- **Bi-directional and physical isolation :** SXN isolates and physically masks the 3 environments
- **Regulatory Compliance :** Architecture certified as compliant by ANSSI (French Cybersecurity Agency)
- **Simplified administration** vs a diode architecture
- **Governance Principle :** separated responsibilities with ½ rules

Nuclear Use Case ®

✳ **Challenge :**
Digitalization of Practices

✳ **Requirements :**
- Protect security and reliability of critical systems while allowing system configuration and software updates
- Sustain systems use that we can't update anymore
- Allow data exchange between networks from different governance models
- **Isolation of a nuclear power plant control center with IT**

✳ **Process :**
- Comparison of several technologies (fw, diode, protocol break application/hardware)

✳ **Selected solution :**
Seclab (hardware protocol break)

Customer benefits :
- **Physical Isolation :** segmentation and segregation network at 100 %
- **Regulatory compliance** : Architecture certified CSPN by ANSSI (French Cybersecurity Agency)
- **Resistant to zero-day :** Attacks protection on network layers and operating system
- **Long time support**

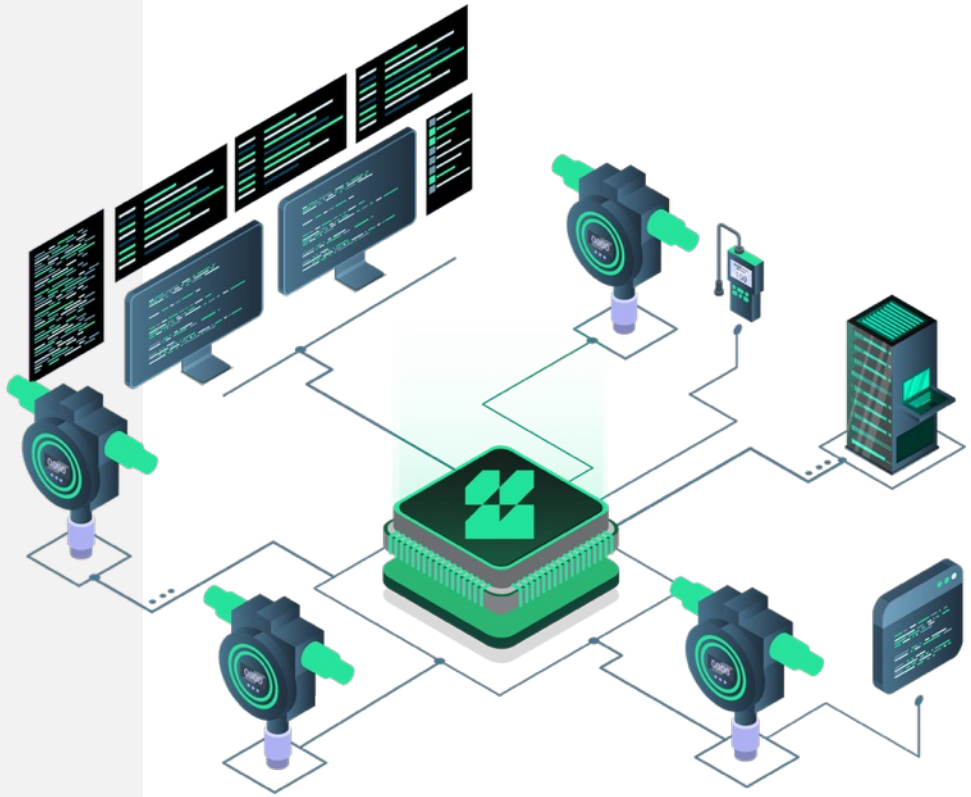
Energy Use Case ®

✳ **Challenge :**
Digitalization of Practices

✳ **Requirements :**
- IT / OT interconnection
- Isolation of interconnection with third parties
- No latency time
- **Bidirectional exchanges between sensors and control center**

✳ **Process :**
- Comparison of several technologies (fw, diode, protocol break application/hardware)
- Validation of isolation level
- Latency time < 1ms

✳ **Selected solution :**
Seclab (hardware protocol break)



Customer benefits :
- **Bi-directional and physical isolation :** SXN isolates and physically masks the 2 environments
- **Regulatory compliance** : Architecture certified at a cyber level and a security level
- **Simplified administration** vs a diode architecture
- **Governance Principle :** separated responsibilities with ½ rules

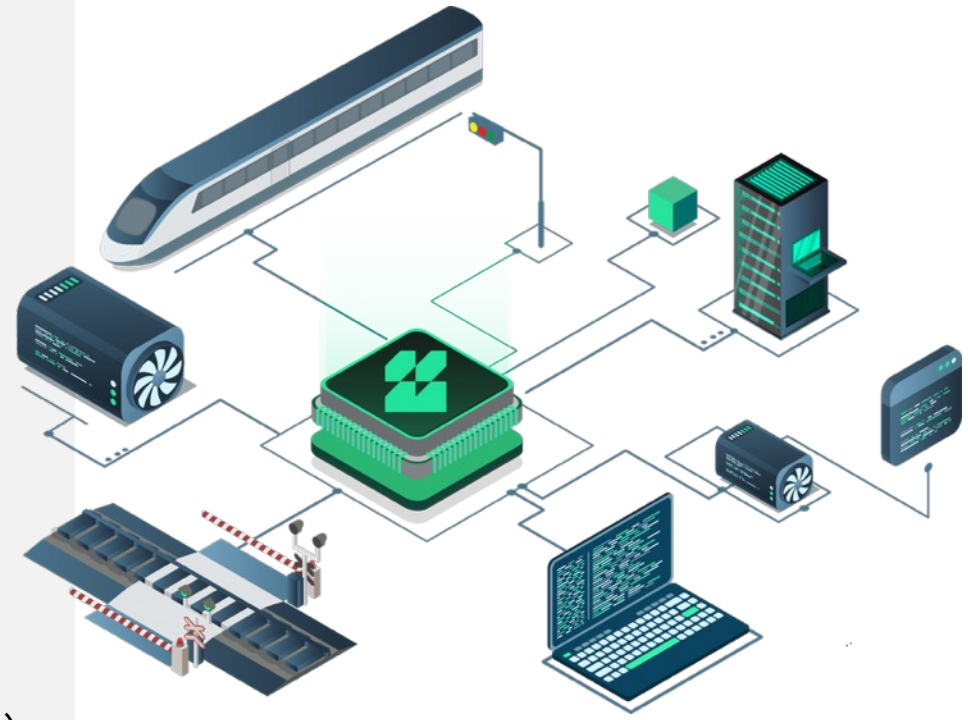
Transport Use Case ®

✳ **Challenges :**
Digitalization of Practices & Opening to competition

✳ **Requirements :**
- IT / OT Interconnection
- Regulatory compliance
- Isolation of interconnection with third parties
- **Isolation between the signaling network and IT network**

✳ **Process :**
- Comparison of several technologies (fw, diode, protocol break application/hardware)
- Validation of the security level with NATO briefcase
- Functional validation of the architecture (application flows)

✳ **Selected solution :**
Seclab (hardware protocol break) + Stormshield (application analysis)



Customer benefits :
- **Physical isolation :** SXN isolates and physically masks the 2 environments
- **ZEHO Regulatory Compliance :** Architecture certified as compliant by ANSSI (French Cybersecurity Agency)
- **Resistant to zero-day :** No dependance on software patches
- **Long time support**

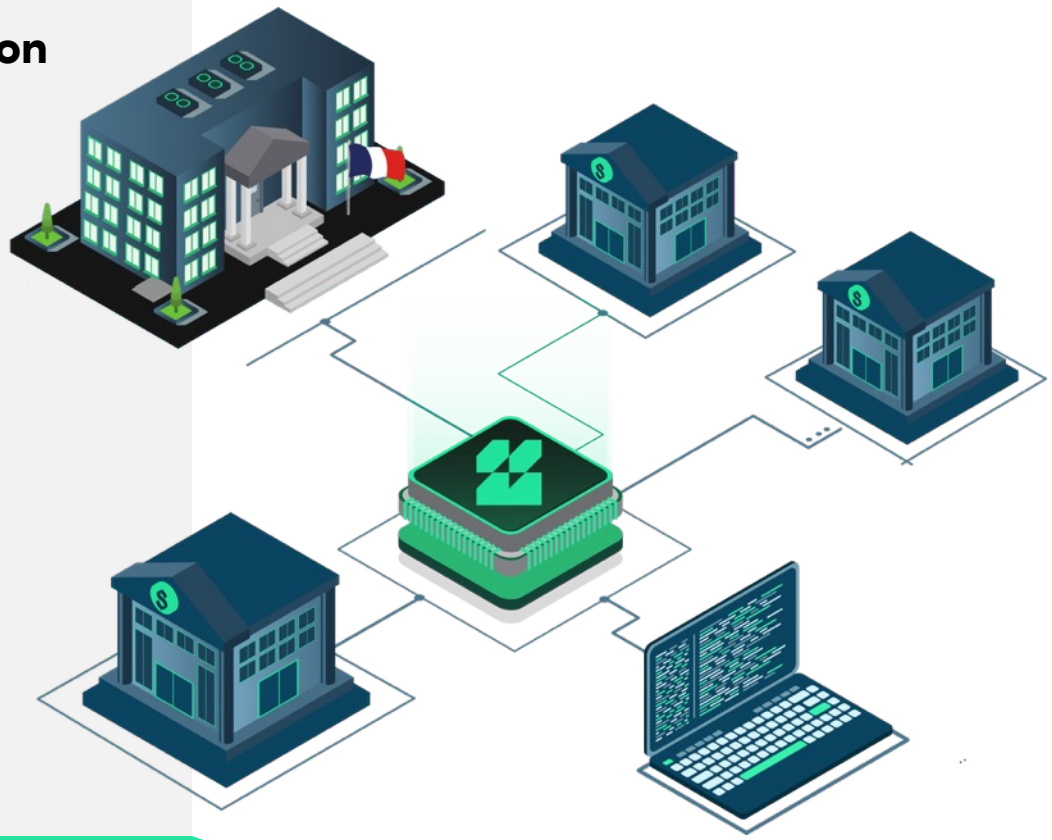
Public Ministry Use Case ®

✳ **Challenges :**
IS controlled opening with third parties & Application isolation from intern network

✳ **Requirements :**
- Opening and **isolation of critical application**
- Physical DLP
- XML file exchange platform
- Securing of communications TCP/IP with third parties

✳ **Process :**
- Comparison of several technologies (fw, diode, protocol break application/hardware)
- Validation of the security level
- Functional validation of physical DLP

✳ **Selected solution :**
Seclab (hardware protocol break)



Customer benefits :
- **Bi-directional and physical isolation :** SXN isolates and physically masks the 3 environments
- **Costs optimization :** Protocol-agnostic solution for traversing protocols
- **Resistant to zero-day :** No dependance on software patches

seclab®

The Cyber-physical systems company

THANK YOU

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