Product datasheet

Xplore.

See-First Intelligence

Xplore.

Visibility, mapping and detection solution for industrial networks and critical infrastructure.

YOU CAN ONLY PROTECT WHAT YOU KNOW

A complete, up-to-date view of the operational infrastructure is required before any industrial cybersecurity program can start. Xplore builds an exhaustive OT asset inventory, maps the flows actually observed and identifies system vulnerabilities.

NON-INTRUSIVE BY DESIGN

Xplore analyzes a copy of the network traffic, with no packet injection and no heavy agent to install. The inventory is completed with lightweight, controlled scripts and executables (SAE). Operations are preserved, including on legacy or fragile equipment.

A PROGRESSIVE MATURITY PATH

A portable audit in a few hours, then continuous mapping and monitoring, then advanced attack supervision. The same software covers all three phases, with no monolithic investment. Data collected on day one feeds the detection baselines.

NON-INTRUSIVE OT DISCOVERY
- Passive traffic analysis
- Controlled data collection

THE MOST COMPLETE OT MAPPING ON THE MARKET
- Logical, Purdue, network, business, geographic views
- Exhaustive flow matrix

AUDIT OR MONITORING MODE
- Mobile deployment
- Fixed sensors, continuous tracking

AI-ENHANCED DETECTION
- 4 complementary engines
- Behavioral analysis
- Contextualized alerts

COMPLIANCE
- NIS2
- IEC 62443

Designed and developed in France.

The Brain

- Real-time centralization and analysis of sensor traffic
- Built-in administration and visualization interface
- Local upload of packet capture files (PCAP) for fully isolated sites
- Built-in alert and vulnerability queues
- Deployed as a physical or virtual appliance

Passive collection sensors

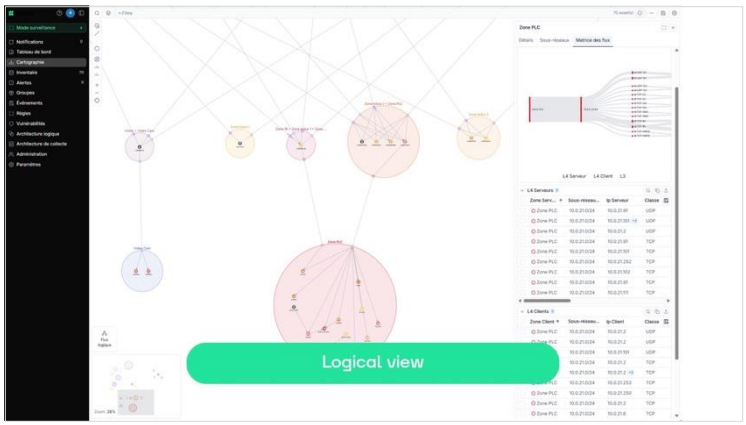
- Hardware or virtual sensors
- Collection via port mirroring (SPAN, RSPAN, ERSPAN) or network TAP
- Traffic copy only, with no interaction with the equipment
- VLAN and GRE tunneling support to relocate the sensor
- IPFIX and NetFlow support
- Listening inside the broadcast domain

Enrichment and isolated sites

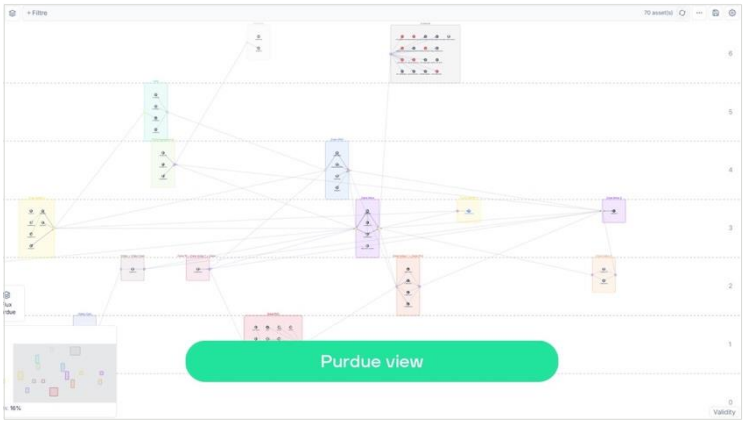
- SAE-N: retrieves asset locations on the physical switch ports
- SAE-S: inventories installed applications, vulnerable software and USB devices
- SAE-dv: enrichment on DeltaV systems
- Collector, a low-cost collection appliance for small isolated or remote sites

Multi-view mapping.

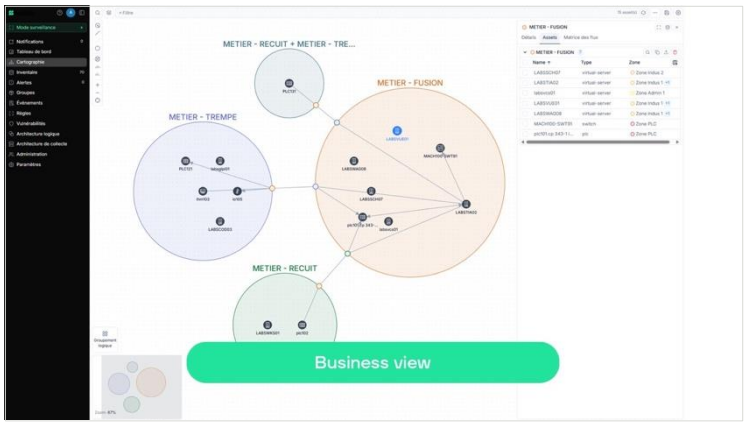
Five native representations of the network, generated from the same data. Each view targets a different audience and exports to Draw.io or Visio.



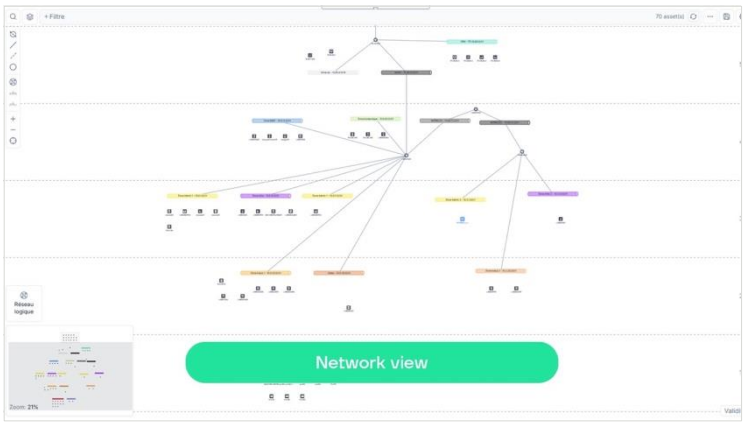
Shows network zones with their assets and the flows between those zones, or between individual assets.



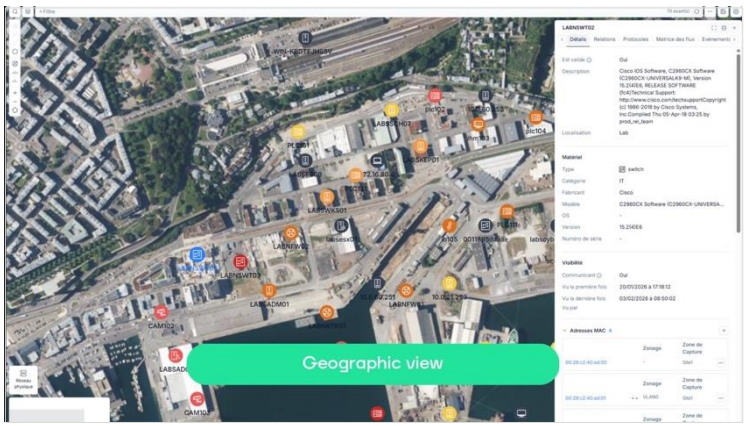
Organizes the map according to the IEC 62443 model. For automation engineers and OT managers.



Creates and displays functional zones tied to the process, for operations teams.



Blends the Purdue view with a classic network topology, including automatic router and firewall detection.



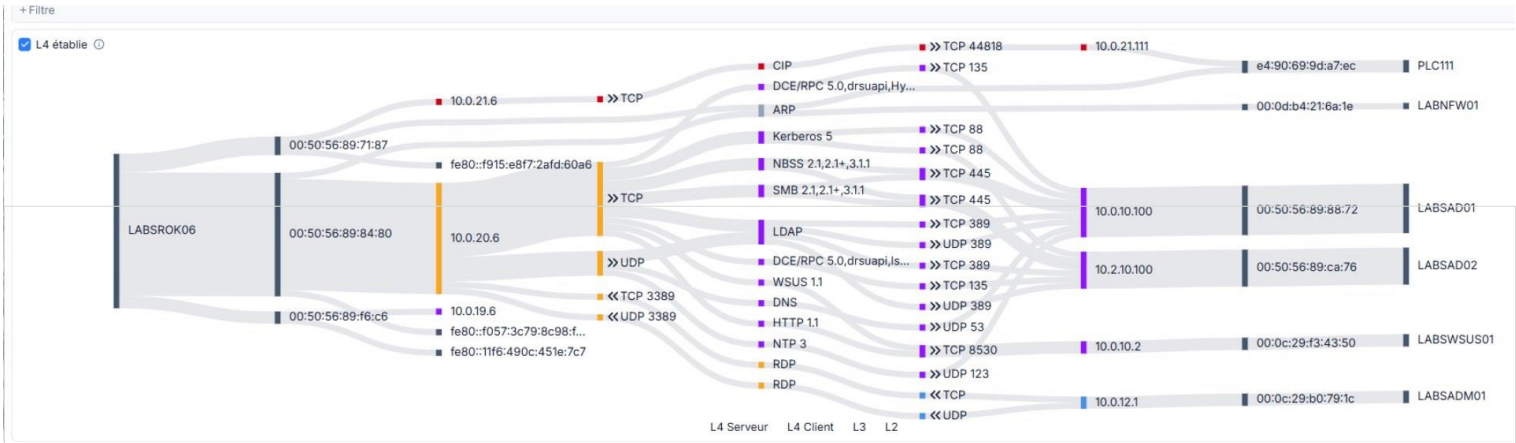
Physically locates critical or vulnerable assets, for site managers and OT leaders.

One dataset, five readings

- All five views are generated automatically or manually from the same dataset
- Xplore works at the network core, on non-routed networks and on isolated perimeters
- Existing firewall and switch configurations can be imported as a reference
- Xplore then separates what is assumed from what is actually observed
- Draw.io and Visio export for migration or remediation projects

Flow matrix

Xplore reports the communications actually observed on the network. For every asset, zone or link, it shows which devices are talking to each other. Protocols appear with the direction of each exchange and the zones involved. The OSI breakdown runs from the data link layer up to the application layer. The flow matrices of each conduit can serve as a basis for regular firewall rule reviews.



Breakdown of one asset's communications, from layer 2 to the application layer, with the direction of each exchange.

Risk management.

Risk-oriented inventory

- Tabular inventory view, sortable and filterable by device type, maintainer, criticality, vulnerabilities, purchase year…
- Risk scored on several criteria: business and operational impact, availability, traceability, recovery priority…
- Vulnerabilities identified from passively collected metadata, or through enrichment
- Vulnerability list shareable with a SOC, a VOC or a vulnerability manager

Attack paths and prioritization

- Vulnerable assets identified by color code on the map
- Realistic attack paths visible directly in the views
- Detection of unauthorized remote access and dual-homed machines
- Contextual patch management, based on the map
- Identification of the vital assets to isolate first, with automatic generation of the Seclab Xchange isolation configuration

Protocols analyzed

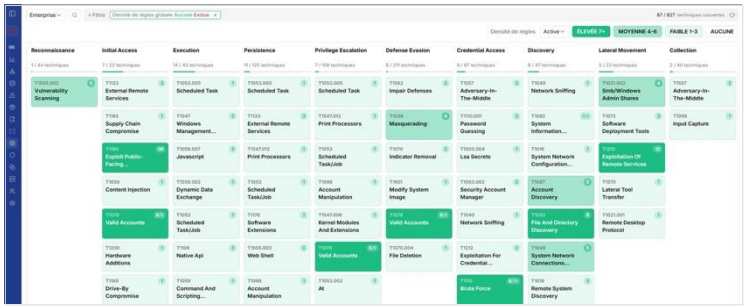
- Standard IT protocols
- Industrial protocols such as Modbus TCP/RTU, S7comm, EtherNet/IP, OPC-DA and OPC-UA, BACnet, DNP3, IEC 60870-5-104, PROFINET and many more.
- Non-routed layer 2 protocols also supported, by listening inside the broadcast domains
- IPFIX and NetFlow

Intelligent detection.

Xplore relies on four complementary detection engines, mapped to MITRE ATT&CK tags to give a synthetic view of detection coverage. The Xplore approach starts from the feared events and the mapping data, to target a rule set that stays relevant and manageable over time.

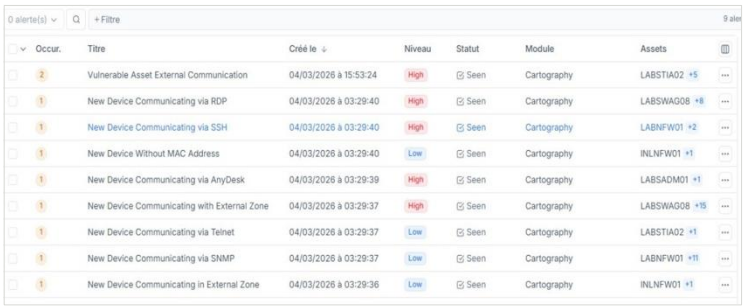
The four detection engines

Cartography-based detection	Monitors the stability of the environment: new devices, configuration changes, unexpected IPv6 addresses, deviations from the baseline, connections to Internet zones. Rules can be built directly from the map.
Sigma signatures	A detection engine based on a format well established in the systems world, extended by Seclab to the network layer. Readable, documentable and annotatable, it stays understandable for OT teams.
Suricata signatures	A Suricata engine runs in parallel. Xplore contextualizes the alert before sending it to the SOC. An IP address alone means nothing to an outside analyst unfamiliar with the plant or the process.
AI behavioral	Machine learning of the network's usual patterns and identification of deviations. Builds on the stability that characterizes industrial environments.



MITRE ATT&CK coverage

Rule density by tactic and by technique, to steer real coverage.



Contextualized alert queue

Every alert carries its assets, its zone and the engine that raised it.

Alerts, routing and forensics

- Standalone alert queue, or forwarding to an external SIEM
- Routing by alert type and criticality to the right recipient
- Continuous traffic recording, with PCAP retrieval from an alert for forensic analysis

Compliance deliverables

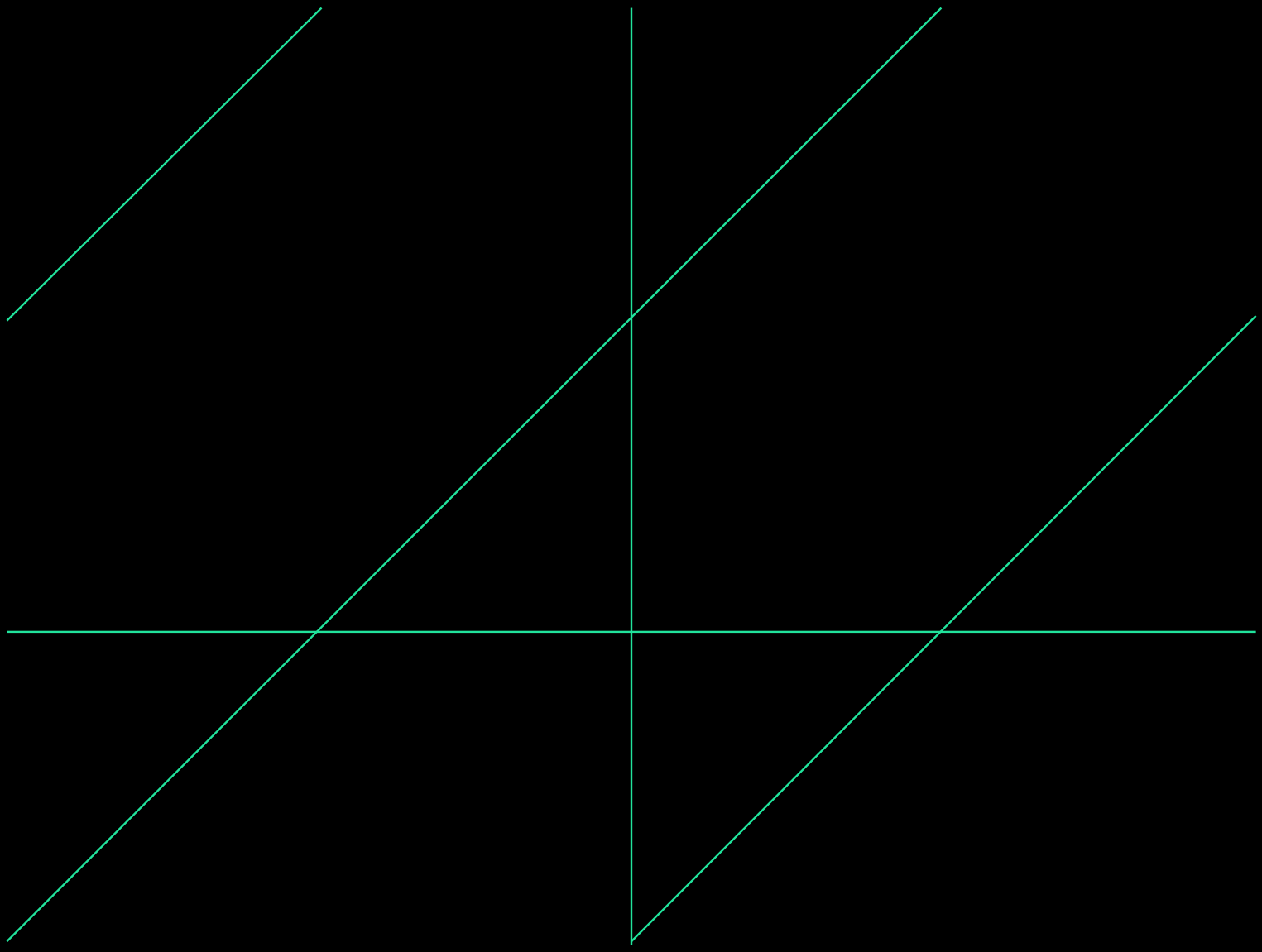
- NIS2: auditable inventory, documented mapping, segmentation analysis, traceability
- IEC 62443: Purdue view, zones and conduits
- French LPM: consolidated audit reports and MITRE ATT&CK coverage

Ecosystem

- Integrations with firewalls, SIEM, SOC, bastion hosts, PAM, IAM, CMDB
- Part of the Seclab Xcore platform, alongside Xchange for physical network isolation and Xport for USB access control.

seclab®

Next-Gen OT
Cybersecurity Platform



205 impasse John Locke
34470 Pérols, France.

seclab-security.com