



100% French and sovereign solution

INDUSTRY

BUILDINGS

SUPERVISION

ENERGY

TRANSPORT

HEALTHCARE

MARINE

LABORATORY



Secure your IoT. Protect your PLCs.

Supermarket refrigeration, industrial PLCs, supervision, heating, access control, energy meters, on-board networks, medical equipment, measuring instruments: these devices run production, buildings and essential services, yet nobody really monitors them.

The WYBOT probe listens to them, learns their habits and reports anything that deviates from them.

What the probe analyses in your traffic.

A PLC always talks to the same workstations, with the same commands, at the same pace. So does a heating controller. WYBOT learns this routine on its own, with no configuration or prior inventory, and notices what changes.

Industry

Factories, workshops, machine tools

New peer for a PLC

A workstation that had never talked to this PLC connects to it.

Write to a PLC

A command that changes a device, from a machine that had never done so. Read on Modbus, DNP3 and EtherNet/IP.

Shop-floor network reconnaissance

A machine querying devices one by one to map them.

Unusual time or transfer

An engineering workstation active at a never-seen hour, or a very large transfer to a PLC (firmware).

Buildings and sites

Building management, heating, access, energy

BACnet and Niagara devices

BMS (Building Management System) controllers are recognised and tracked, each with its own habits.

New device plugged in

An unknown device appears and responds on the technical network.

Device talking to the Internet

A controller exchanges with a never-seen Internet server.

Unusual relationship

A workstation that had never talked to a controller connects to it. More serious at night.

Supervision and processes

Supervision workstations

OPC UA traffic from a workstation that never connects to it.

Instrumentation

A never-seen workstation exchanges with a HART-IP instrument.

Energy and metering

Substations and telecontrol

DNP3 or IEC 104 traffic from a source missing from the history.

Meters and tanks

A new peer queries a meter or a tank gauge.

Transport

On-board network

TRDP or SOME/IP traffic outside the usual exchanges.

New device

An unknown device appears on the on-board network.

Healthcare

Imaging

An imaging device exchanges with a rarely seen Internet server.

Usual servers

A device steps outside its usual servers (PACS, RIS, HL7 gateway).

Measuring instruments

A never-seen workstation exchanges with an instrument (HiSLIP).

Marine

Navigation

A new transmitter (GPS, AIS, compass) appears, or a transmitter reaches out to the Internet.

Retail

Commercial refrigeration

Controllers of refrigerated display cases and cold rooms are recognised and tracked, each with its own habits.

New peer

A workstation that had never talked to a refrigeration plant connects to it. More serious at night.

Recognised protocols.

WYBOT identifies them automatically based on their content, their port, their behaviour, or a combination of these criteria. You have no list to maintain and no indicator to send us

AUTOMATION AND MACHINES

Modbus Modbus UMAS Siemens S7 S7CommPlus
EtherNet/IP (CIP) PROFINET Omron FINS Beckhoff ADS
GE EGD GE SRTP Saia Ether-S-Bus Saia EtherSIO PCWorx
Red Lion Mitsubishi MELSEC Mitsubishi MELSOFT CODESYS
Triconex TriStation

SUPERVISION AND PROCESSES

OPC UA HART-IP DDS-RTPS (robotics) PTP (clock)

ENERGY AND METERING

DNP3 IEC 104 IEC 61850 MMS IEEE C37.118 IEC 62056 (DLMS)
ANSI C12.22 Tank gauges (ATG)

BUILDINGS AND CONNECTED DEVICES

BACnet KNX LonWorks Niagara Fox MQTT CoAP

TRANSPORT

TRDP (rail) SOME/IP (automotive) CAN over IP

HEALTHCARE

DICOM (imaging) HL7 v2 (patient records)

MARINE

NMEA 0183 (navigation) IEC 61162-450 Navico radar

LABORATORY

HiSLIP (instruments)

Four situations, caught in time.

An attack on an industrial site or a building rarely starts with the PLC. It first goes through a workstation, a remote access or a forgotten device. Each step leaves a trace that the probe links to the others.

INDUSTRY

The maintenance contractor's laptop

A technician plugs his laptop into the shop-floor network for a service call. The laptop is infected and starts exploring nearby machines.

WYBOT ANALYSES:

- 01 Traffic from a device missing from the network history
- 02 Successive traffic to several PLCs, a possible sign of reconnaissance
- 03 Traffic to a PLC this device has never contacted

LEVEL

Medium

Alert before any write: the team unplugs the laptop.

INDUSTRY

A PLC reprogrammed remotely

A supervision workstation may be remotely controlled by a third party. This workstation then sends a Modbus write command to a PLC on the line.

WYBOT ANALYSES:

- 01 Remote-control traffic outside usual time slots
- 02 Modbus traffic carrying a write command, a first for this workstation
- 03 Deviations from the usual exchanges of this production PLC

LEVEL

Critical

The case file names the workstation, the PLC and the traffic involved.

BUILDINGS

A BMS reachable from the Internet

A heating controller was opened to the Internet during commissioning, then forgotten. Bots start probing it.

WYBOT ANALYSES:

- 01 The controller responds to traffic coming from the Internet
- 02 Repeated traffic, at all hours

LEVEL

Medium

The exposed controller is identified before it is changed.

BUILDINGS

An unknown BMS workstation in the middle of the night

At 3 a.m., a workstation that had never talked to a building's heating controller connects to it over BACnet.

WYBOT ANALYSES:

- 01 BACnet traffic from a never-seen workstation to this controller
- 02 Night time for the site (10 p.m. to 7 a.m.)

LEVEL

Medium

The facility manager checks first thing in the morning whether work was scheduled.

A clear alert, at the right level.

On a production site, an alert must say at once whether action is needed. Each kind of finding has a weight; a machine's level is their sum over 24 hours. The same finding repeated adds nothing.

1 LOW A machine on the technical network sends more data than usual, with no other sign.	2 MEDIUM An office workstation exchanges with a PLC for the first time.	3 HIGH This workstation also calls back, at a regular pace, an unknown Internet server.	4+ CRITICAL The same workstation sends a Modbus write command to the PLC.
--	---	---	---

The report stays cautious: it states what was seen and what it may mean. It never asserts an attack without evidence.

What you receive

One case file per machine

All findings about a machine are grouped together, in the order they appeared.

A plain-language report

Short sentences, no jargon, understandable by a site manager as well as a technician.

The checks to carry out

For each alert: which device, which workstation, which protocol, and what to check on site.

A view of all your sites

Factories, warehouses and buildings on one screen, from the most urgent to the calmest.

Zero noise. WYBOT first learns the site's habits for 14 days. Industrial detections then start in observation mode: they are counted without appearing in the report. For each customer, a detection that has stayed quiet for 21 days (at most one alert) activates on its own.

Shall we look at your PLCs together?

Ask for a demo on your own data. One week is enough for a first assessment.



Let's talk about your cybersecurity.

Ask for a demo on your own data. One week is enough for a first assessment.

WYBOT Cybersécurité

45 avenue du Général Leclerc
76120 Le Grand-Quevilly, France

+33 2 32 18 23 54

wybot-cybersecurite.com
