



Complete Visibility of Legacy PLCs and Industrial Assets

One plant on paper.

Three plants worth of network underneath.



DISCOVER

See every legacy PLC
and network device



MAP

Uncover hidden
connections



VERIFY

Validate inventory
with confidence



UNDERSTAND

Gain accurate insight
across all assets



A pharmaceutical manufacturer running tablet compression, coating, and liquid filling lines across two connected buildings engaged Shieldworkz after realizing its OT asset inventory predated two plant acquisitions. The engagement built an accurate, current picture of every legacy PLC and network device without disrupting validated production systems.

THE CHALLENGE

Manufacturing plants that grow through acquisition often inherit more network than anyone documented. Each new line brings its own switches, its own PLC vendor, and its own history, and over time nobody in plant engineering can say with certainty what is actually connected.



No Current Inventory

The last full asset list was three years old and predated a plant acquisition.



Unknown Network Paths

Two acquired lines were tied into the network without updated documentation.



Regulatory Deadline

A NIST CSF alignment review required asset-level evidence the plant could not produce.



Turnover Risk

Engineers who understood the original network design had since left the company.



Validation Constraints

GxP validation rules meant systems could not be actively scanned or touched.

Use Case Overview

Build an accurate, current inventory of every PLC, HMI, and network device across both buildings without touching validated systems or interrupting batch production.

SHIELDWORKZ SOLUTION HIGHLIGHTS



Passive Asset Discovery

Switch-level sensors identified devices without querying controllers directly.



Asset Classification

Devices cross-checked against validation records to confirm what each one controlled.



Network Mapping

Undocumented paths from both acquired lines traced into one diagram.



Protocol Documentation

Modbus RTU, OPC UA, and PROFINET traffic mapped to the historian.



Vulnerability Review

Unsupported OS and firmware flagged without active scanning.

Risk Prioritization

Legacy systems ranked by exposure and criticality, not age alone.



Compliance Mapping

Findings mapped against NIST CSF to close the audit's gaps.



Governance Handover

Inventory delivered in a format engineering could keep current.



Segmentation Roadmap

Zones proposed for a follow-on phase based on discovery findings.



Monitoring Recommendation

Baseline traffic documented to support a future detection phase.



HOW IT WORKED



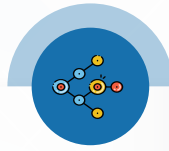
Discover

Passive sensors installed at core switches in both buildings over two weeks.



Classify

Every device cross-checked against existing qualification and validation paperwork.



Map

Network paths between the two acquired lines documented into one architecture view.



Prioritize

Legacy and unsupported systems ranked by exposure and process criticality.



Handover

Inventory and findings delivered with an update process for plant engineering.

BUSINESS OUTCOMES

- 500+ industrial assets identified across two connected buildings, most absent from the previous inventory
- Roughly 40% of discovered devices had no prior documentation tying them to plant records
- Full network architecture diagram produced, covering paths added during both plant acquisitions
- NIST CSF asset-management gaps closed ahead of the compliance review
- Legacy and unsupported systems ranked and handed to plant engineering for phased replacement planning
- Baseline traffic patterns documented to support a future continuous monitoring phase



Shieldworkz Threat Research Lab Insight

OT asset visibility remains one of the biggest challenges in industrial cybersecurity. Our assessments consistently find legacy PLCs, unmanaged devices, and undocumented network connections that increase operational risk and delay incident response.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through classification, mapping, and prioritization under one team.



OT-Specific Expertise

Engineers who understand PLCs, DCS, and batch processes, not just IT inventory tools.



Validation-Aware Method

Discovery respects GxP validation boundaries instead of treating every system as scannable.



Standards-Based Approach

Findings mapped directly against NIST CSF and other recognized frameworks.



Built for Regulated Plants

Documentation delivered in a form that supports FDA and other regulatory review.



About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations



Security Operations Center



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!



From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us



GERMANY



- 📍 Fritz-Schäffer-Street 1,
4th floor
Bonn, 53113, Germany
- ☎ +49 (0) 228 / 929 39210
- ✉ europe@shieldworkz.com

CANADA



- 📍 396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada
- ☎ +1 (437) 223-7770
- ✉ americas@shieldworkz.com

UAE



- 📍 Tenth floor,
Abu Dhabi,
United Arab Emirates,
FAB Business Center
- ☎ +971 56 660 5200
- ✉ middleeast@shieldworkz.com

INDIA



- 📍 Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli
- Bengaluru,
Karnataka 560093
- ☎ +91 9059620557
- ✉ apac@shieldworkz.com

