SHIELDWORKZ

USE CASE | Manufacturing Industry

IEC 62443
Compliance Across Multiple Plants

Three plants. Three histories.
Three operations, one level of secure meant.

UNIFIED One standard.
CONSISTENT Same approach.
OVERSIGHT Live view.
AUDIT READY Prove compliance.

A packaging manufacturer operating a corrugated converting plant, a flexible film extrusion plant, and an injection-molded closures plant needed to show a consistent security posture across all three sites ahead of a cyber insurance renewal. Each plant had grown independently, with different PLC vendors, different network designs, and no shared baseline. The engagement built one maturity baseline and a phased roadmap across all three locations.

THE CHALLENGE

Manufacturers that grow through separate plant leadership, regional expansion, or acquisition often end up with as many security philosophies as they have sites. Each plant manager solves problems locally, and nobody above them can say how the sites compare.

No Shared Baseline
Each plant defined its own security posture with no common way to compare them.

Insurance Deadline
A cyber insurance renewal required documented evidence of a framework at every site.

Mixed Maturity
One site ran industrial firewalls and managed switches another still used unmanaged switches.

Local Decision Making
Each plant's engineering manager set priorities independently with no shared budget process.

Inconsistent Audit History
Findings from an audit at one plant had no bearing on what the others could show.

Use Case Overview
Assess all three plants against the same IEC 62443 maturity model, prioritize findings across the portfolio, and build one governance framework and roadmap instead of three separate ones.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Multi-Site Gap Assessment
IEC 62443 assessed independently at each plant against the same maturity model.

Asset Discovery
Passive inventory run at each site to establish what was actually in place.

Cross-Site Risk Prioritization
Findings ranked together so leadership could compare risk across all three plants.

Phased Monitoring Rollout
Continuous monitoring sequenced starting with the least mature site.

Common Zone Model
One architecture pattern adapted to each site's specific layout.

Vulnerability Assessment
Legacy Windows systems and unsupported firmware flagged at each location.

Segmentation Roadmap
Zoning planned per plant but built toward the same target state.

Security Awareness Training
Delivered consistently to engineering teams across all three plants.

Unified Governance
One policy set replacing three separately defined sets of rules.

Executive Reporting
Consolidated maturity scoring built for leadership and insurance documentation.

HOW IT WORKED

Discover

Asset and architecture review carried out independently at each of the three plants.

Assess

IEC 62443 gap assessment applied using the same maturity model at every site.

Prioritize

Findings ranked across all three plants into one combined list.

Govern

A shared policy set and decision process defined to replace local rules.

Deploy

Segmentation and monitoring rolled out site by site, starting with the highest risk.

BUSINESS OUTCOMES

- All three plants assessed against a single IEC 62443 maturity baseline for the first time
- Consolidated findings gave leadership one prioritized list instead of three disconnected reports
- A unified governance policy adopted across all sites, replacing locally defined rules
- Segmentation roadmap defined per plant, built toward a shared target state
- Insurance renewal supported with consistent documentation across all three locations
- Security awareness training delivered to engineering staff at every plant

Shieldworkz Threat Research Lab Insight

Multi-site OT assessments consistently reveal significant differences in security maturity, governance, and network architecture across plants. A common IEC 62443 framework enables organizations to measure risk consistently, prioritize investments, and build a unified cybersecurity program.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through governance, prioritization, and rollout under one team.

OT-Specific Expertise

Engineers who understand plant-floor realities, not just framework checklists.

Standards-Based Approach

Assessment and roadmap built directly on the IEC 62443 maturity model.

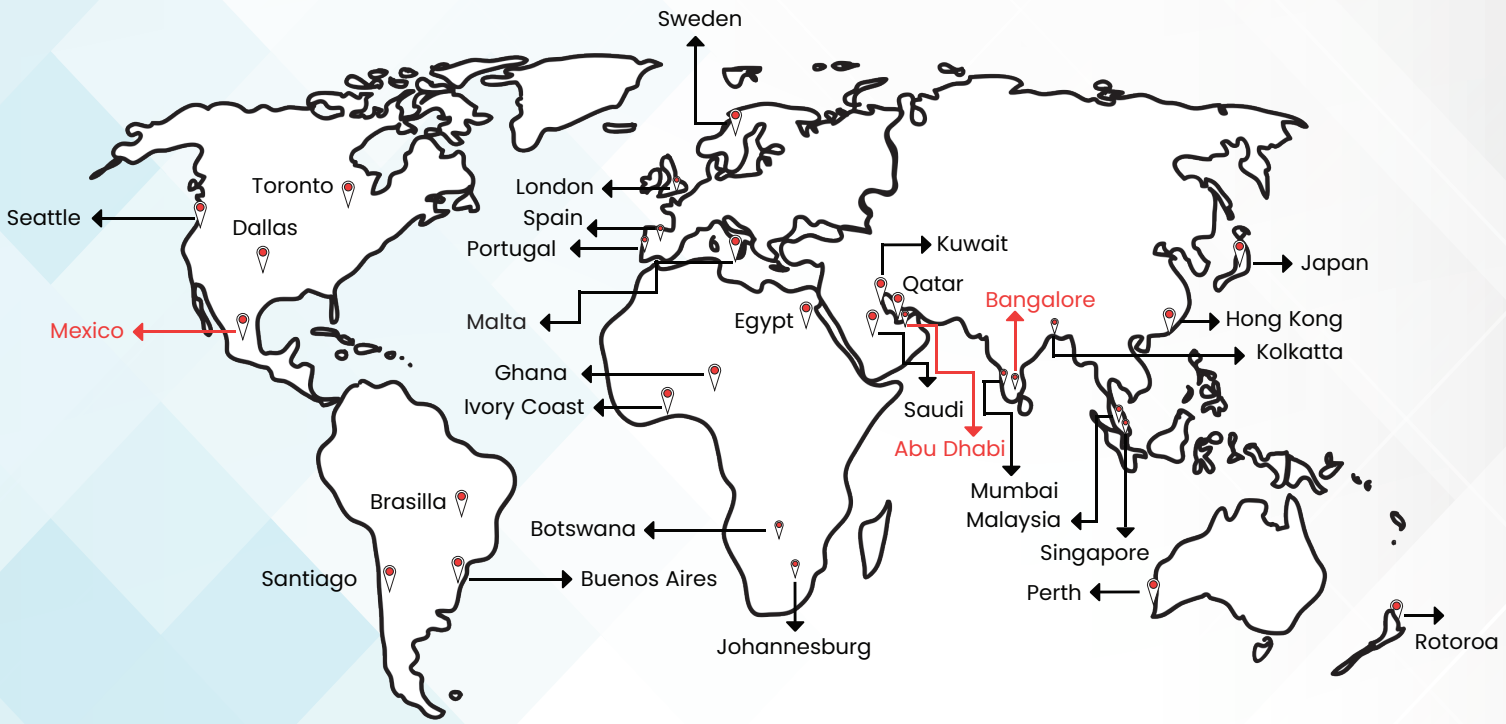
Multi-Site Experience

Programs designed to scale consistently across plants with different histories.

Built for Executive Reporting

Findings consolidated into a form leadership can act on portfolio-wide.

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