SHIELDWORKZ

USE CASE | MANUFACTURING INDUSTRY

OT Security Operations Center for 24x7 Monitoring

The furnace never stops.
The monitoring **couldn't either.**

- 24x7 Threat Monitoring
- Real-time Incident Detection
- OT Asset Visibility
- Continuous Risk Assessment
- Rapid Response & Mitigation

A glass container manufacturer running a continuous furnace and three forming and inspection lines had one engineer responsible for OT security alongside other network duties. Existing tools generated alerts, but nobody reviewed them outside business hours, and a weekend anomaly on the furnace control network went unnoticed until Monday. The engagement stood up 24x7 monitoring and response without requiring the plant to build its own around-the-clock team.

THE CHALLENGE

Continuous-process plants don't get downtime windows, and neither can their security coverage. When monitoring depends on one person being at their desk, whatever happens outside that window simply doesn't get seen until someone gets back to it.

One-Person Coverage
A single engineer covered OT security alongside other network duties.

No After-Hours Review
Alerts piled up unreviewed through nights, weekends, and holidays.

Furnace Never Stops
Continuous 24/7 furnace operation left no safe window for gaps in monitoring.

Weekend Anomaly Missed
A furnace network anomaly went unnoticed until the following Monday.

Single Point of Failure
Vacation, illness, or turnover meant zero coverage on any given day.

Use Case Overview
Stand up around-the-clock monitoring and response for the furnace and forming line networks, with an escalation path built for this plant rather than generic IT alerting.

24x7 OT SOC
Analysts monitor the plant's OT network around the clock, not just business hours.

Incident Response Support
Help containing and investigating anything the SOC surfaces.

Furnace-Specific Context
Analysts trained on what normal furnace and forming line traffic looks like.

Threat Intelligence
Focused on the specific ICS vendors and equipment in use on-site.

Passive Asset Discovery
Visibility baseline the SOC uses to tell normal from anomalous.

Continuous Monitoring
Removes dependency on any one person being available around the clock.

OT Threat Detection
Tuned specifically to the furnace DCS and forming line PLC networks.

Alert Tuning
Detection rules calibrated over time to reduce noise without missing events

Defined Escalation Path
The engineer is only contacted for confirmed, relevant events.

Governance Reporting
Regular reporting gives leadership visibility into coverage and findings.

HOW IT WORKED

Discover

Asset and network visibility baseline established across furnace and lines.

Onboard

SOC analysts trained on the plant's specific architecture and normal behavior.

Tune

Detection thresholds calibrated to reduce noise while catching what matters.

Define

A clear escalation path built between SOC detection and plant response.

Monitor

24x7 coverage goes live, with rules refined against real alert history.

BUSINESS OUTCOMES

- 24x7 monitoring coverage established for the first time across furnace and forming line networks
- After-hours and weekend alert gaps closed
- Mean time to detect anomalies on the furnace control network reduced from days to minutes
- The plant's single OT engineer freed from constant alert triage, escalated only for confirmed events
- A documented escalation process now connects SOC detection to plant response
- Monitoring coverage extended without the plant needing to staff an internal SOC team

Shieldworkz Threat Research Lab Insight

OT threats don't follow business hours. In our threat investigations, delayed alert reviews and limited after-hours visibility consistently extend detection time and increase operational risk. Continuous 24x7 monitoring helps identify critical events before they disrupt industrial operations.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through detection, escalation, and response under one team.

OT-Specific Expertise

Analysts who understand furnace and forming line context, not generic IT alerts.

True 24x7 Coverage

Monitoring that doesn't stop when the plant's own team goes home.

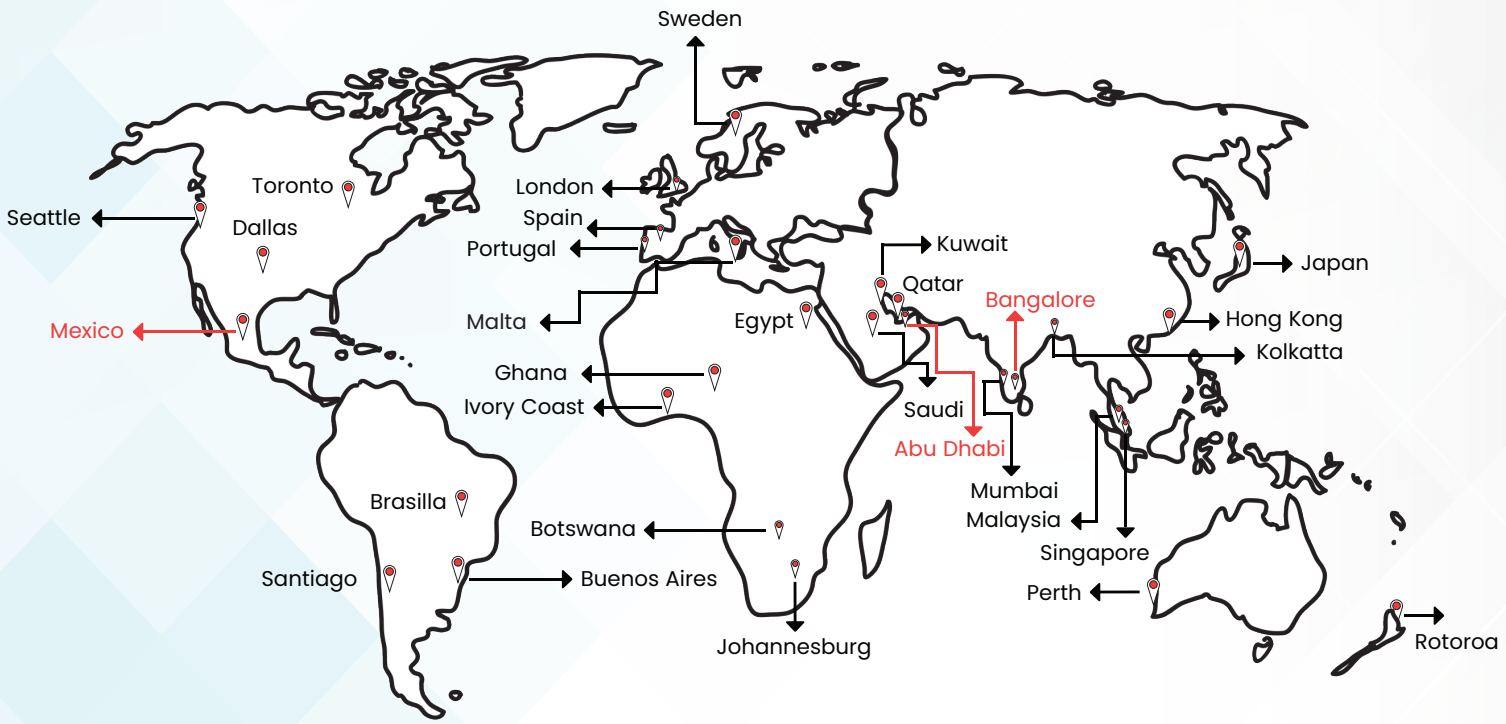
Standards-Based Approach

Monitoring and response aligned to recognized OT security operations practices.

Escalation Built for the Plant

Alerts routed based on what actually matters to this furnace and these lines.

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