

Preventing Ransomware From Shutting Down Production Lines

Contained on IT.

One network hop from the plant floor.



CONTAIN

Keep threats contained within IT.



ISOLATE

Prevent lateral movement.



DETECT

Identify malicious activity early.



PROTECT

Ensure continuity and resilience.

A tier-1 automotive component manufacturer engaged Shieldworkz after a ransomware infection on its corporate IT network came within one hop of reaching the plant floor. The engagement built visibility into the OT network, separated it from IT, and put detection in place without interrupting scheduled production.

THE CHALLENGE

Manufacturers are increasingly targeted by ransomware operators looking to disrupt operations and force a payout. Once malware reaches the OT network, it can halt PLCs, corrupt recipe and configuration data, and stop a line mid-shift.



No Asset Visibility

Security could not assess exposure because the OT network had never been inventoried.



Unmonitored Vendor Access

A shared remote desktop ran on standing credentials with no session logging.



Compliance Pressure

Two OEM customers began requiring IEC 62443 evidence with no documentation on file.



Aging Firmware

Stamping line PLC firmware had not been reviewed in several years



Downtime Exposure

A ransomware event was estimated at four to six hours of downtime per line.

Use Case Overview

Give plant engineering full visibility into the OT network, separate it from corporate IT, and put detection and response in place without interrupting scheduled production.

SHIELDWORKZ SOLUTION HIGHLIGHTS



Asset Visibility

Passive sensors built a full inventory of PLCs, HMIs, the historian, and workstations.



Network Segmentation

OT isolated from IT behind a dedicated firewall, lines split into separate zones.



Continuous Monitoring

PROFINET and Ethernet/IP traffic baselined to flag anomalies in real time.



Secure Remote Access

Standing vendor credentials replaced with time-bound, logged sessions.



Vulnerability Management

PLC firmware and workstations reviewed to prioritize patching by exposure.



Compliance Alignment

Practices assessed against IEC 62443 to produce OEM audit documentation.



Threat Detection

Alerts tuned against real plant traffic rather than generic signatures.



Incident Response Planning

Alerts tuned against real plant traffic rather than generic signatures.



Security Governance

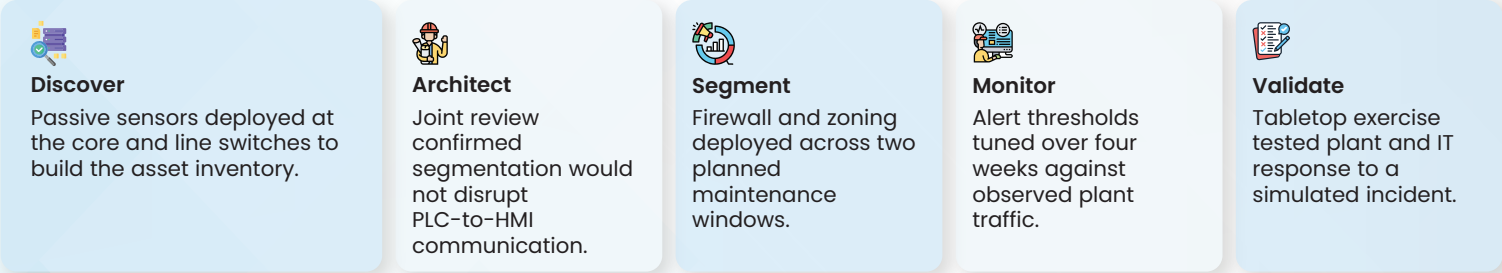
Findings and remediation tracked for ongoing compliance reporting.



Monitoring Handover

Alert thresholds and escalation paths handed to plant staff to run day to day.

HOW IT WORKED



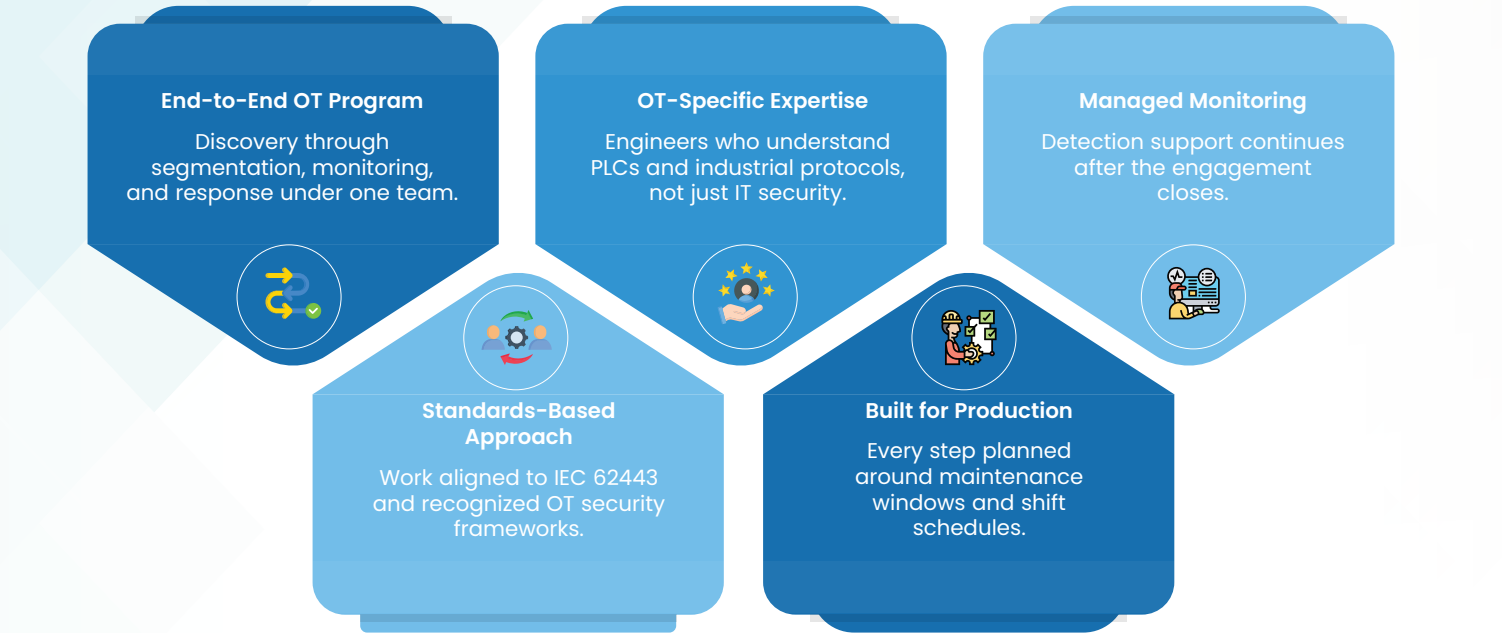
BUSINESS OUTCOMES

- 340+ OT assets identified and inventoried, including devices plant staff were not previously aware of
- Full network visibility achieved across both production lines within the first three weeks
- Vendor remote access converted from standing shared credentials to logged, time-bound sessions
- High-priority vulnerabilities reduced by roughly 60% following the first coordinated patch cycle
- OT network isolated from corporate IT through dedicated firewall segmentation and line-level zoning
- IEC 62443 gap assessment completed and documentation delivered ahead of the OEM audit deadline
- Anomaly detection time reduced from an untracked, manual process to under 15 minutes

We finally know what is connected to our network, and we can see when something changes. That is the difference between catching an issue in minutes and losing a shift.

Plant Engineering Manager, Automotive Component Manufacturer

WHY SHIELDWORKZ



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

