



Detecting Cyber Attacks on Compressors and Pumping Stations

An operator happened to notice.
That was the entire detection strategy.



Detect Anomalous Behavior



Monitor OT Traffic in Real-Time



Identify Unauthorized Access Early



Correlate Events for Faster Response



Ensure Continuous Operational Visibility

A crude oil gathering operator running six pump stations between wellpad tank batteries and a central terminal noticed unusual VFD speed changes at one station that did not match dispatcher commands, caught only because an operator happened to be watching the SCADA trend at the time. Investigation found unauthorized traffic reaching the station's PLC, with no automated way it would otherwise have been detected. The engagement built detection that does not depend on someone happening to be watching.

THE CHALLENGE

A pump station a hundred miles from the nearest control room does not stop being a target just because nobody is standing next to it. It just means whatever happens there depends entirely on whether anyone is watching the right screen at the right moment.



No Automated Detection

The one incident caught depended entirely on an operator noticing a trend.



Unattended Remote Stations

Most pump stations sat unmonitored between periodic technician visits.



Shared Telemetry Network

Radio telemetry connected all stations without separation between them.



Custody Transfer Exposure

Tampering with volumetric data carried direct financial and contractual risk.



No Repeatable Strategy

Leadership could not accept an operator noticing by chance as an ongoing plan.

Use Case Overview

Replace an operator noticing a mismatched trend with automated detection at every pump station, segmented so an event at one site cannot silently reach the others.

SHIELDWORKZ SOLUTION HIGHLIGHTS



Per-Station Asset Discovery

Visibility extended individually to all six pump stations.

Risk Prioritization

Stations ranked by remoteness and consequence of an undetected event.



Command Baseline

Normal dispatcher-to-station traffic established for comparison

Incident Response Planning

Safe verification steps defined before any pump station restart.



OT Threat Detection

Flags command or setpoint changes that don't match dispatch instructions.

Governance Reporting

Detection findings tied to both safety and custody transfer integrity.



Telemetry Segmentation

Shared radio network divided so one station's anomaly can't reach another.

Vulnerability Review

PLC and VFD firmware reviewed for exposure at each station.



Continuous Monitoring / OT NDR

Coverage at unattended stations, day or night.

Validation Testing

Detection confirmed against a simulated unauthorized command.



HOW IT WORKED



Discover

PLC, VFD, and telemetry traffic mapped at each of the six pump stations.



Baseline

Normal dispatcher-to-station command traffic established.



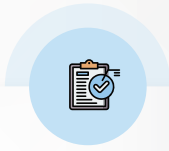
Segment

Shared telemetry paths between stations separated.



Detect

Command and setpoint activity that doesn't match dispatch flagged automatically.



Validate

Detection tested against a simulated unauthorized command before go-live.

BUSINESS OUTCOMES

- Automated detection in place across all six pump stations, removing dependence on manual trend-watching
- Unauthorized or unexplained command activity now flagged in near real time
- Shared telemetry network segmented so an event at one station stays contained and visible
- Stations ranked by risk, giving the most remote sites priority attention
- A validated response plan in place for a pump station event, including safe restart verification
- Detection capability documented and tied to both safety and custody transfer integrity reporting



Shieldworkz Threat Research Lab Insight

Remote pumping stations rarely fail because attackers are highly sophisticated—they fail because no one is watching. Across industrial OT environments, our threat research consistently shows that unattended assets, legacy PLCs, and shared telemetry networks create the longest detection gaps, allowing unauthorized activity to persist until operators notice operational anomalies.

WHY SHIELDWORKZ

End-to-End OT Program

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



OT-Specific Expertise

Engineers who understand pump station and VFD control, not just generic SCADA.



Detection Beyond the Control Room

Coverage extended to remote, unattended stations, not just where an operator watches.



Standards-Based Approach

Detection and response aligned to recognized OT security operations practices.



Built Around Consequence

Stations prioritized by how much damage an undetected event could actually cause.



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

