SHIELDWORKZ

USE CASE - RENEWABLE ENERGY

Bringing Consistent OT Monitoring to a Distributed Solar Portfolio

A curtailment command meant for one site reached inverters at a plant sixty miles away, and nobody could say why for two days.



FULL VISIBILITY | THREAT DETECTION | NETWORK SECURITY | REAL-TIME ALERTS | COMPLIANCE & REPORTING

A renewable energy operator running a portfolio of utility-scale solar plants from a central operations center found that a curtailment command intended for one site was executed at a different plant entirely. The investigation showed the operations center reached each site's SCADA and inverter network through a different, largely unlogged path. Shieldworkz built a consistent baseline across the portfolio and gave the operations center one governed way to reach any site.

THE CHALLENGE

Every site had monitoring. What the portfolio lacked was one consistent way to see, reach, and trace activity across all of them.

Inconsistent Site Architectures

Each plant used a different OEM SCADA and inverter monitoring platform, with no common visibility standard across the portfolio.

Unlogged NOC-to-Site Access

The operations center reached site networks through a mix of VPNs and vendor portals with no consistent session logging.

Cross-Site Command Exposure

A misrouted curtailment command reaching the wrong plant showed that site networks weren't as isolated as assumed.

No Command-Level Monitoring

Dispatch and curtailment commands to inverters left no record of source, timing, or destination site.

Emerging NERC CIP Exposure

As aggregate portfolio capacity grew, several sites approached thresholds that would bring new compliance obligations.

Use Case Overview
Give the operations center one governed, logged way to reach every site, and add monitoring that can trace any dispatch or curtailment command back to its source and destination plant.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery
Inverters, combiner boxes, tracker controllers, and SCADA platforms mapped across every site in the portfolio.

OT Vulnerability Assessment
Inverter and SCADA firmware reviewed across the portfolio, prioritized by site criticality and interconnection size.

Portfolio-Wide Segmentation
Each site's SCADA and inverter network isolated from the others, closing the path that let one plant's command reach another.

Multi-Protocol Visibility
Communication with substation relays, meters, and inverters normalized into a single monitoring view across OEM platforms.

Secure Remote Access
Operations-center-to-site connections consolidated into a single broker with per-site scoping and full session logging.

NERC CIP Readiness Assessment
Documentation and controls prepared for sites approaching compliance thresholds.

OT NDR & Continuous Monitoring
Traffic at each site watched against a baseline built from normal inverter and tracker communication.

OT SOC & Managed Monitoring
Alerts from every site routed to one team instead of separate OEM dashboards.

Command-Level Traceability
Dispatch and curtailment commands tied to a specific operator, session, and destination site.

Portfolio Onboarding Governance
A standard process defined for bringing new sites onto consistent monitoring from day one.

HOW IT WORKED



Discover

Inverters, combiner boxes, and SCADA platforms mapped across every site in the portfolio.



Segment

Each site's network isolated from the others, closing the path between plants.



Consolidate Access

NOC-to-site connections unified into one broker with per-site scoping.



Baseline & Tune

Normal inverter and tracker communication baselined, alerts calibrated per site.



Monitor

Portfolio-wide activity handed to the managed OT SOC for ongoing review.

BUSINESS OUTCOMES

- Inverters, combiner boxes, and SCADA platforms mapped across all 14 utility-scale sites in the portfolio
- Operations-center access consolidated from multiple vendor VPNs and portals into one governed broker
- Command-level traceability established for dispatch and curtailment activity across every site
- The cross-site command path that misrouted the original curtailment command permanently closed
- Monitoring coverage now consistent across all OEM platforms through a single operations view
- NERC CIP documentation prepared for the sites nearing compliance thresholds

Shieldworkz Threat Research Lab Insight

Shieldworkz Threat Research Lab's telemetry shows that expanding connectivity across remote OT sites, wireless devices, and connected control systems is creating new blind spots for industrial operators. With threat intelligence drawn from 50,000+ honeypots and wireless s ensors, the research highlights how attackers increasingly exploit remote and connected OT environments. For distributed solar portfolios, consistent monitoring, segmentation, and command-level traceability are therefore critical to prevent activity at one site from becoming an operational risk across the portfolio.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through segmentation, access consolidation, and ongoing monitoring under one team.

Distributed Portfolio Expertise

Experience monitoring multi-site renewable assets, not just single-plant environments.

Multi-Vendor Normalization

One monitoring view built across inverter and SCADA platforms from different OEMs.

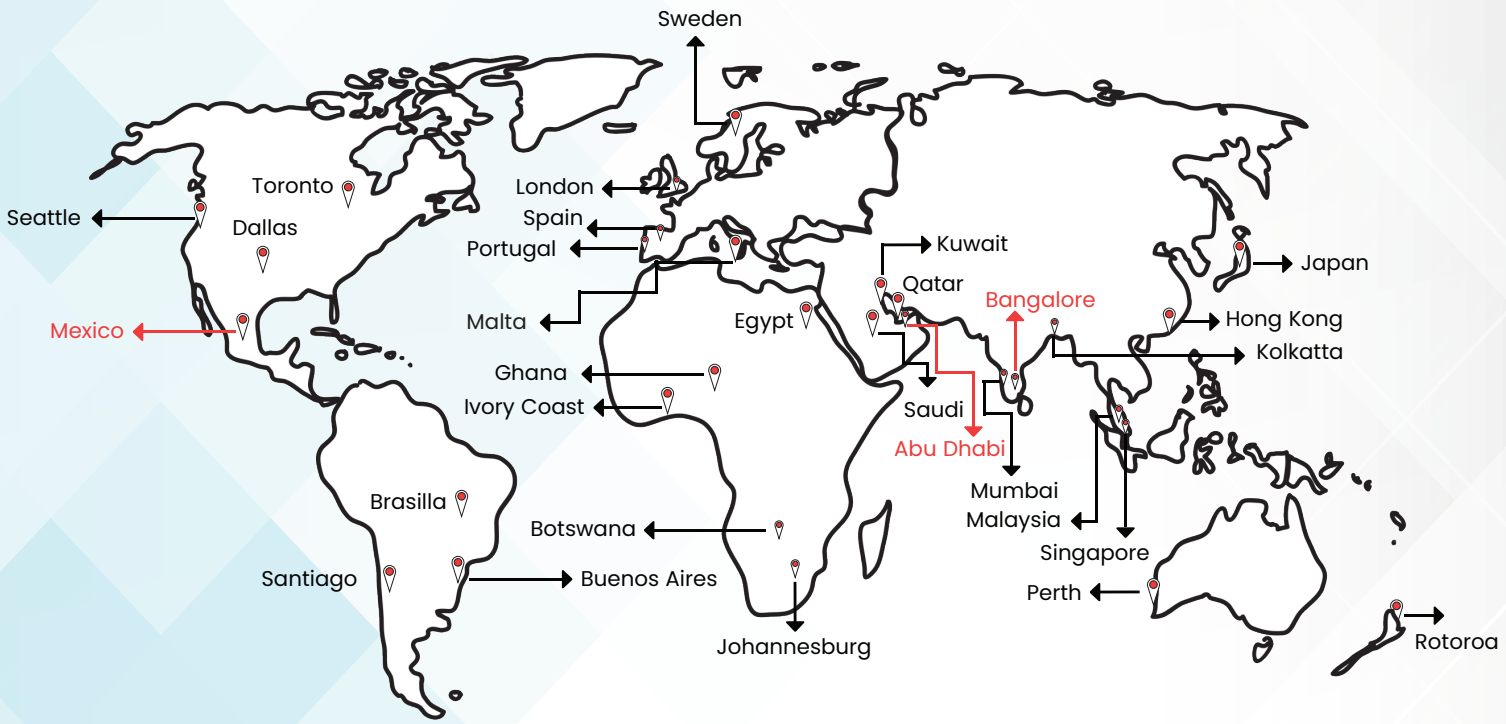
Standards-Based Approach

Segmentation and access governance aligned to IEC 62443 and NERC CIP practice.

Managed OT SOC

Ongoing monitoring handed to a team that watches OT traffic across the whole portfolio.

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.

Copyright @ 2026, Shieldworkz - All rights Reserved.

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

Copyright @ 2026, Shieldworkz - All rights Reserved.