Case Study 3: Non-Intrusive OT Monitoring Deployment for Critical Infrastructure (Municipal Water District end customer)

Objectives: Deploy and configure an OT (Operational Technology) security platform with passive sensors to monitor assets and baseline network activity. Tune alerts, enable snapshots, and train the OT team for ongoing monitoring and future scaling.

Delivery Format/Duration: Remote/3 weeks

Client Overview

Leading cybersecurity firm, publicly-traded

End Customer Overview

Municipal Water District (MWD) delivers critical water, wastewater, and recycled water services to hundreds of thousands of residents across its county. With a large geographical footprint and multiple operational sites, MWD manages a range of industrial control systems (ICS) across its OT environment. Recognizing the increasing threat landscape targeting municipal infrastructure, MWD took a proactive step to gain visibility into its OT assets and network activity by deploying an OT Security tool.

The goal was to passively monitor control system traffic, baseline normal behavior, and begin establishing a robust security posture—without interfering with the operational continuity of water services.

Engagement Objectives

- **Deploy OT Security Core and four passive sensors** to capture traffic across MWD's plant facilities
- **Discover and classify OT assets** across diverse control system vendors and subnets
- **Establish initial policy baselines** to tune alerting, reduce false positives, and highlight true anomalies
- **Enable active querying and snapshot capabilities** for prioritized asset types
- **Empower MWD's OT security team** through hands-on configuration, tuning, and roadmap planning

Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131

Phone:
+1 (786) 397-0480

Maill:
info@cyopspartners.com

Strategic Priorities

- **Non-Disruptive Deployment in Live OT Environments:** With water delivery and wastewater treatment being essential 24/7 services, MWD prioritized passive data collection to avoid operational risk during implementation.
- **Accurate OT Asset Inventory:** Leadership wanted a detailed, real-time map of devices across plants—including PLCs (Programmable Logic Controllers), HMIs (Human-Machine Interfaces), and RTUs (Remote Terminal Units)—without relying on manual asset spreadsheets or vendor documentation.
- **Reduction of Alert Fatigue:** Security staff required assistance tuning the security tool's policies so that alerts reflected meaningful deviations rather than normal ICS (Industrial Control Systems) communications.
- **Controller Insight and Policy Coverage:** The team wanted to begin using active queries and snapshots selectively to gain configuration-level visibility and prepare for future compliance needs.
- **Enablement and Future Scalability:** With limited in-house OT cybersecurity experience, the engagement needed to serve as both a technical deployment and a training milestone to prepare the team for ownership and future maturity milestones.

Approach

Our team executed the engagement over three weeks, combining structured remote delivery with active collaboration. The steps are aligned to a five-phase deployment methodology. We were engaged by the vendor to lead this deployment on their behalf.

1. Planning and Infrastructure Validation

- Reviewed MWD's OT architecture and confirmed monitoring points across three regional sites.
- Guided the collection of SPAN (Switched Port Analyzer) data using Wireshark to verify clean packet capture and validate visibility at each plant.
- Assisted with static IP assignment and validated firewall rules for inter-device communication on TCP ports 28303 and 28304.

2. Deployment and Version Hardening

- Installed and configured the OT Security Console and four remote sensors, one per region.
- Upgraded the software version and walked through appliance configuration: hostname, DNS, NTP, and user access roles.
- Verified sensor telemetry and traffic flow in the Core dashboard, with connectivity and health monitoring enabled.

3. Asset Discovery and Traffic Classification

- Within 48 hours, the OT Security tool identified:
    - 1,891 OT assets, including controllers from vendors like Rockwell and Siemens
    - Network protocols including Modbus, DNP3, and proprietary industrial protocols
- Assets were classified by type, firmware version, communication behavior, and assigned to plant-specific Monitored Asset groups.
- 89 vulnerabilities were identified—none associated with inbound internet traffic, confirming a segmented but exposed architecture.

4. Alert Policy Tuning and Asset Enrichment

- Two baseline policies were modified to reduce alert volume related to expected east-west traffic.
- Custom policies were configured for detecting:
    - Unauthorized outbound traffic
    - Controller behavior anomalies
    - Potential misconfigurations
- Active querying was selectively enabled to retrieve controller metadata and perform snapshot configuration baselines on critical devices, timed to avoid operational windows.

5. Roadmap and Knowledge Transfer

- Delivered a tailored roadmap with near-term and long-term recommendations:
    - **Baseline Establishment:** Allow sensors to observe uninterrupted network behavior for several weeks before tightening policy thresholds
    - **Scheduled Active Queries:** Run snapshots during maintenance windows to avoid potential strain on older controllers
    - **Platform Expansion Planning:** Explore integration with the Vulnerability Management Console for unified IT/OT dashboards
    - **Training Path:** Encourage use of training resources like courses on OT Security operations and incident handling
    - **Health Check in 6–12 Months:** Plan for a formal optimization review once baseline maturity is achieved

Results & Impact

- **Complete OT Visibility Within Days:** MWD gained comprehensive awareness of its industrial environment, replacing manual inventory methods with live, detailed device-level insights.
- **Tuned Alerting for Operational Clarity:** Initial policy baselining helped reduce noise while preserving visibility into events that warranted investigation.
- **Foundation for Governance and Reporting:** The snapshot functionality and controller queries provided MWD with valuable input for future integrity checks and compliance efforts.
- **Skilled Internal Team Ownership:** MWD's OT and cybersecurity personnel directly configured the platform, guided by interactive coaching—building in-house confidence to sustain and expand the deployment.
- **Clear Path to Maturity:** With sensors deployed, alerts operational, and a growth roadmap in place, MWD is now positioned to scale its OT security efforts across additional sites and integrate into broader IT/OT initiatives.

End Customer Feedback

"This engagement gave us the tools and visibility we needed to finally understand what's happening inside our Operational Technology networks. The deployment was smooth, the tuning helped filter the noise, and the roadmap sets us up for success."

— **OT Security Program Lead**, Municipal Water District

Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131

Phone:
+1 (786) 397-0480

Maill:
info@cyopspartners.com