InfoSight®
www.infosightinc.com



Control the unseen, turn your OT network into a defensible system

24X7 OT & ICS THREAT MONITORING & Managed Detection & Response (MDR)

Industrial control environments were built for reliability, not cyber-resilience. Flat networks, untracked firmware, and unmonitored PLC communications let attackers manipulate process logic before anyone notices. InfoSight's MDR for OT provides centralized visibility, risk analytics, and continuous human oversight across every SCADA and OT segment—turning unmanaged exposure into measurable control.

www.infosightinc.com info@infosightinc.com 305-828-1003

Architecture & Standards Alignment

Compliance is the baseline; resilience is the outcome.

Evidence generation mapped to IEC 62443, NERC CIP, and TSA directives. Architectural awareness aligns to ISA-95 and the Purdue Model (Level 0–5), with segmentation context preserved in detections and reporting.

U.S. critical-infrastructure focus aligned to CISA Cross-Sector Cyber Performance Goals (CPGs) for objective control maturity and board-level assurance.

Non-Disruptive Integration

Traffic is mirrored only. No taps placed inline, no agents on PLCs, no changes to cycle times. Engineering change windows aren't required. Control latency remains unchanged; safety interlocks remain authoritative.

CORE VISIBILITY CAPABILITIES

Deep Asset Discovery: Find every PLC, HMI, RTU, engineering workstation, and historian. Capture device type, model, serial, firmware, and communication relationships. Parse industrial protocols including Modbus/TCP, PROFINET, CIP (EtherNet/IP), BACnet, and DNP3 to validate live process context.

Behavioral Analytics: Baseline operational behavior and surface process deviation and engineering workflow anomalies—not just timing or policy drift. Detect maintenance outside approved windows, off-hour changes, and command sequences that don't match normal procedures.

Control-Process Language (CPL): Detect unexpected write commands to PLC registers, unauthorized firmware downloads, ladder/logic edits, and unsafe mode changes. Highlight who changed what, where, and when—with replayable evidence.

Passive Threat Detection: Mirror traffic from existing switches. No inline components. No impact on control latency. Identify malicious behavior and lateral movement using mirrored OT telemetry—operations remain untouched.

Scalable Design: Start at a pilot site and expand across plants, substations, and geographies. Support multi-zone/segment rollouts without re-architecting.

Unified SOC View: Aggregate every monitored site into InfoSight's U.S.-based, SOC 2-certified operations center for 24×7 monitoring, investigation, and escalation.

TRANSFORM VISIBILITY INTO CONTROL — CONTINUOUS OT DEFENSE THAT THINKS LIKE AN OPERATOR



What You Get:

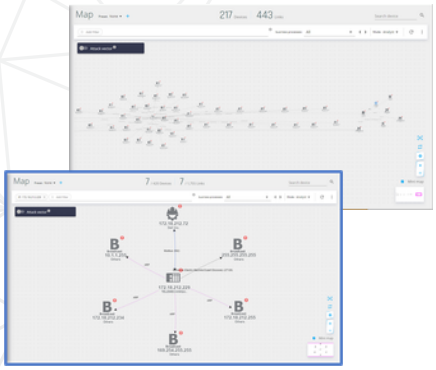
- **Passive Threat Monitoring at Scale:** Smart collectors mirror live traffic to the iSID analytics core for non-intrusive detection.
- **Centralized Analytics Dashboard:** Correlates global threat intelligence with localized OT telemetry for prioritized response.
- **Live Network Mapping:** Auto-discovers and visualizes process communication paths for every site and subnet.
- **Configuration Integrity Tracking:** Validates every firmware change, patch, and engineering update to ensure process safety.
- **Multi-Tiered Implementation:** InfoSight manages full deployment—including shipping, configuration, and training—with local teams empowered to complete remaining sites.
- **Turn-Key Success:** Includes all ancillary equipment and accessories required for end-to-end delivery.

PROVE IT: QUANTIFIED RISK & CONTINUOUS ASSURANCE

Each deployment concludes with a Cyber Industrial Automated Risk Analysis (CIARA) assessment that:

- **Maps vulnerabilities (CVSS/CVE-based).**
- **Runs breach attack simulations using MITRE-ICS frameworks.**
- **Quantifies business impact and risk-reduction priorities.**
- **Generates a regulatory-aligned compliance report with actionable mitigation roadmap.**

This transforms traditional post-incident review into continuous, data-driven OT risk intelligence.



THE INFOSIGHT EDGE — HUMAN JUDGMENT WHERE AUTOMATION ENDS

- ***25 years securing critical infrastructure and regulated industries.***
- ***100 % U.S.-based, SOC 2-certified analysts—no outsourcing, no bots.***
- ***Co-managed SOC model extends, not replaces, your engineering team.***
- ***Proven record across energy, manufacturing, utilities, and water sectors.***

Fewer false positives. Faster validation. Measurable resilience.

Predict • Detect • Contain • Restore — Driven by Experts Who Understand the Process Behind the Packet.

TAKE THE NEXT STEP

Know your exposure. Quantify your operational risk.™

InfoSight's 24X7 OT & ICS THREAT MONITORING & MDR delivers continuous visibility, measurable assurance, and peace of mind for every critical control network you operate.