InfoSight®
www.infosightinc.com

# 24X7 OT & ICS THREAT MONITORING & INCIDENT RESPONSE

305-828-1003 info@infosightinc.com

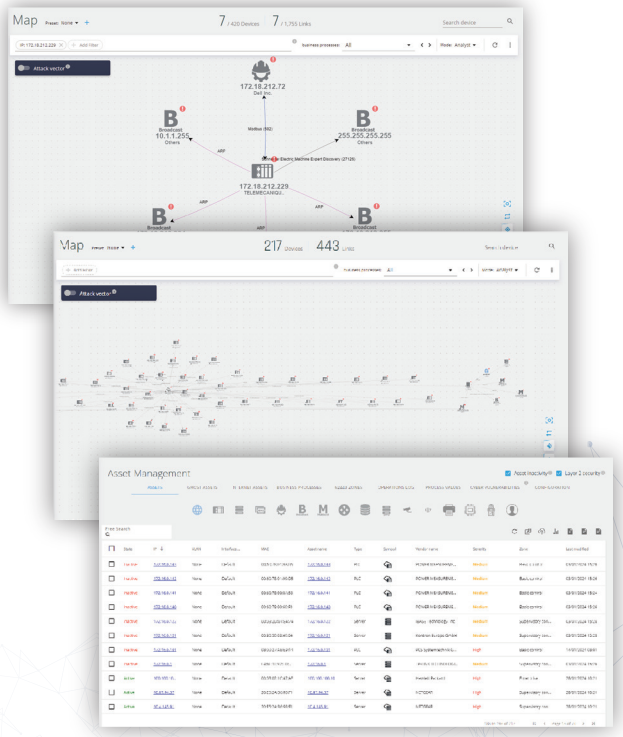
## The Challenge

Today, OT & ICS Networks have become a prime target for state-sponsored attackers. Vulnerabilities within Legacy Networks, along with partial asset inventories cause a lack of threat visibility making identifying threats almost impossible in some cases. Additionally, the lack of security tools, change management tracking and limited or no reporting just compound the problem. And as part of our Nation's critical infrastructure with an expanding threat landscape, impending regulatory requirements are on the horizon. Attackers work 24x7, while most organizations OT departments don't... Additionally, tight cybersecurity budgets and the effort required to analyze all security events can be exhausting leading to employee fatigue and turnover. Recruiting and retaining cybersecurity analysts is probably the most challenging it has been in decades. Your team should be focused on more strategic objectives that support business goals and not fighting cybersecurity fires.

## Overview

We provide non-disruptive monitoring of distributed SCADA networks for changes in topology and behavior, using multiple security packages, each offering a unique capability pertaining to a specific type of network activity:

- **Network Visibility –** Using passive scanning of all OT network traffic, we create a visual dynamic network map for all devices, protocols and sessions, with alerts upon detected topology changes. (e.g. new devices or sessions.)
- **Cyber Attack –** The Cyber Attack package handles known threats to SCADA network, including PLCs, RTUs and industrial protocols, based on data gathered from across the cyber security research community.
- **Policy Monitoring –** Define/modify policies for each network link, for validating specific commands (e.g. "write to controller") and operational ranges (e.g. "do not set turbine to above 800 rpm.")
- **Maintenance Management –** Limit network exposure during scheduled maintenance by creating work orders for specific devices during set time-windows. A log report of all maintenance activities is issued upon session completion.
- **Asset Management –** Presents all system assets, categorized and filterable by type (e.g. PLC, Server, HMI, Engineering Station, Broadcast, etc.) or by any asset characteristic. Asset types are automatically detected, and the user can change each asset's designation or add a custom asset type.
- **Anomaly Detection –** The Anomaly Detection feature creates a behavioral network model using multiple parameters, including device sequence sampling time, frequency of operational values and more, toward detecting behavioral anomalies.
- **Operational Behavior –** Monitor and audit the management of devices (PLC, RTU & IED) at remote sites, with alerts for firmware changes or configuration modifications (e.g. software updates or turning edge devices on or off) and activity logging.



InfoSight®
www.infosightinc.com

# 24X7 OT & ICS THREAT MONITORING & INCIDENT RESPONSE

## How We Deliver It

InfoSight brings a co-managed approach to OT security monitoring by becoming an extension to your OT Security Team to monitor your most critical assets and data sources 24x7x365. Services Include:

- 24X7 Monitoring, Threat Detection & Incident Response
- Incident/Problem Management
- Ongoing monitoring enhancements
- Global Threat Intelligence
- Reporting

## Why InfoSight® ?

24x7x365 Staffed SOC

100% US based SOC 2 Certified Operations Center

Only US-based W2 employees

Providing both Security and Network Infrastructure Support

Support for Cloud, Datacenter or Hybrid networks

Monitoring of Applications, DBs, Security, Infrastructure, Server or Serverless

Offering Device-based or consumption-based pricing models

24x7 or off-peak 7pm-7am coverage available

Federally regulated and critical infrastructure client experience

Cyber liability insurance coverage

24+ years of successful outcomes

## Use cases include:

**Technician on-site** will automatically monitor maintenance activities during the predefined time window. Operations outside of the maintenance boundaries will trigger alerts.

**Unauthorized PLC configuration** changes will detect known protocol commands which affect PLC configuration.

**SCADA server attack** will detect and alert upon changes in the industrial model, including command sequence and timing anomalies in the command sequence and timing.

**Spyware** will generate alerts upon malware attempts to ex-filtrate sensitive data from operational networks. Spyware activity indicators include anomalous network behavior, usage of unknown protocols and establishing of external connections.

**Man-in-the-Middle** will detect and alert upon rogue devices in the network impersonating a valid server, workstation or SCADA controller, by means of Mac or IP address theft.

**Industrial-tailored malware** will identify and alert upon all known tailor-made ICS malware, based on data gathered from across the cyber-security research community. Detection of unknown malware is done based on indications of unauthorized SCADA commands as well as specific anomalies in the industrial process.