LSI listens

Compliance Support

Framework Standards

- **NIST 800-82**
- **ISA-99/IEC-62443**
- **NIST Cybersecurity Framework (CSF)**
- **American Water Works Association (AWWA) G430 Standard**

Industry/Federal Regulations

- **NERC CIP, North American Electric Reliability Corporation – Critical Infrastructure Protection**
- **FERC, Federal Energy Regulatory Commission**
- **CFATS, Chemical Facility Anti-terrorism Standards**
- **AWIA, America's Water Infrastructure Act**

Contact LSI

Let's start a conversation. Call or email our ICS/OT Cybersecurity experts today.

877-735-6905

info@logicalsysinc.com

The Growing Threat of Cyberattacks

Securing OT (Operational Technologies) and ICS (Industrial Control Systems) Networks Against Both Internal and External Threats, Intentional or Accidental

Manufacturers are continually looking for ways to improve their production efficiency, reduce cost and waste, and monitor quality to confirm standards are met. As a result, the world's manufacturing facilities embrace the adoption and deployment of technologies that connect more and more assets and devices to their networks. The benefits of collecting data for timely and clear reporting, or leveraging analytics to uncover process trends and predict manufacturing yields and equipment failure, can be huge. A connected enterprise also presents risks to the manufacturing facility, its employees, and potentially the public if the network and its OT assets are not secure. In fact, many experts in this field believe that it's not a matter of "if" a cybersecurity incident occurs, but "when."

The technology now deployed in OT environments and the risks they are exposed to have many similarities to that seen in IT / enterprise environments. However, understanding the many significant differences between OT and IT environments (e.g., priorities) and the unique and evolving security threats to OT must be considered when designing, implementing, and maintaining a cybersecurity program for an ICS/OT environment and the Critical Infrastructure sectors.

Services and Support

- Assessments & Auditing
  - Security Audit / Gap Analysis based on ICS Standards and Regulations (e.g., CFATS, FERC, NERC-CIP)
  - Vulnerability Assessment (e.g., NIST 800-82, ISA/IEC-62443, NIST CSF, CIS-20)
  - Risk & Resiliency Assessment and Remediation
  - ICS/OT Network Assessment
- Design/Architect OT Network
  - Industrial DMZ
  - Zone Partitioning
- Develop Security Policy and Procedures
- ICS Device Hardening (e.g., Switches, Routers, Computers, etc.)
- OT Cybersecurity Training
- ICS/OT Vulnerability and Penetration Testing
- Threat Detection / Network Monitoring

How We Work — LSI Listens

To support our clients' cybersecurity needs, LSI's team of experts starts by listening, learning, and understanding our clients' processes and business drivers. By combining that understanding with our knowledge and experience of ICS/OT cybersecurity frameworks, industry regulations, and acceptable practices to assess the environment's cybersecurity posture, we can implement the needed remediation. The result is a custom solution, tailored to the needs of that client's process and environment, that reduces the attack surface and hardens the environment against cyber threats.

www.logicalsysinc.com

03272023