UTSI INTERNATIONAL

OT CYBERSECURITY BUILT FOR INDUSTRIAL OPERATIONS

As industrial operations become increasingly connected, cybersecurity has evolved from an IT concern to a business-critical operational priority. Protecting industrial control systems requires more than technology, it demands deep operational expertise, proven methodologies and a partner who understands the balance between cybersecurity, safety, reliability and uptime.

Why It Matters

50% Organizations experienced cybersecurity intrusions impacting OT systems in 2025.

43% Of OT/ICS assets are outdated.

5 : 1 For every five engineers retiring, only one new engineer enters the workforce.

CITGO

Joe Carroll, CIO, CITGO

"UTSI has been a trusted partner in helping us strengthen our cybersecurity program and helping us mature our approach to protecting critical systems. I recommend UTSI to organizations looking for a knowledgeable, practical, and collaborative partner in OT cybersecurity."

Operational resilience depends on securing aging infrastructure while enabling the next generation of industrial operations.

41+

41+ Years

Trusted by critical infrastructure organizations.

Operational First

Cybersecurity strategies designed around safe, reliable operations.

Vendor Agnostic

Solutions driven by client needs—not technology preferences.

Full Lifecycle Support

From assessments through implementation and ongoing operational support.

Cybersecurity is most effective when it strengthens operations — not disrupts them.

A PRACTICAL APPROACH TO OT CYBERSECURITY

Every organization is at a different stage of its OT cybersecurity journey. UTSI provides practical, outcome-focused services that help organizations assess risk, strengthen resilience, improve compliance and align IT and OT around a common goal: protecting critical operations.

Five Critical Capabilities for Strengthening OT Cybersecurity

Tabletop Exercises

Prepare Before an Incident Occurs

Validate response readiness through realistic scenarios that strengthen decision-making, improve cross-functional coordination, and identify opportunities to enhance resilience before a cyber event impacts operations.

Incident Response Planning

Respond with Confidence

Develop practical response and recovery plans that minimize operational disruption, clearly define roles and responsibilities and improve organizational preparedness.

Framework Assessments

Understand Your Current State

Evaluate OT cybersecurity maturity, identify vulnerabilities, benchmark against industry frameworks and prioritize improvements that reduce operational risk.

Regulatory Compliance

Stay Ahead of Requirements

Support compliance with industry cybersecurity regulations and standards while strengthening governance and reducing organizational risk.

IT/OT Convergence Assessments

Bridge the Gap Between IT and OT

Evaluate organizational and technical readiness for secure IT/OT convergence, helping teams align around shared priorities, governance and operational resilience.

Featured Client Success

Strengthening OT Cybersecurity for a Leading Refinery



Challenge
Improve OT cybersecurity maturity while aligning executive leadership around future cybersecurity investments.

UTSI Solution
Delivered AI-powered tabletop exercises that brought together IT, OT, engineering and executive stakeholders to evaluate operational risk, identify capability gaps and develop a prioritized cybersecurity roadmap.

Measurable Outcomes

- Elevated OT cybersecurity maturity from Level 1.5–2.0 to Level 2.5–3.0
- Improved executive understanding of operational cyber risk
- Strengthened IT/OT collaboration and decision-making
- Supported board approval for future cybersecurity investment

Ready to Strengthen Your OT Cybersecurity Strategy?

Partner with UTSI to define the next step in your OT cybersecurity journey.

utsi.com

281 480 8786

@UTSIInternational

Shaun Six
President, CEO
+1 832 208 0028
shaun.six@utsi.com

Frank Benton
Business Development
+1 832 633 0458
frank.benton@utsi.com