**FOR IMMEDIATE RELEASE**

**MEDIA RELEASE**

**MAY 5, 2026**

# Oil and Gas Operators Are Confident They Can Detect a Cyberattack. The Tools They Are Using Cannot. Tosi Reports.

*Independent Tosi survey of 100 U.S. upstream and midstream OT decisionmakers finds 87 percent confident in 24-hour breach detection, but only 16 percent have the OT monitoring to support that confidence.*

**Oulu, Finland / Irving, Texas** – An independent survey of 100 OT decision makers at U.S. upstream and midstream oil and gas operators, conducted for Tosi, finds the sector responding to the post Operation Epic Fury threat environment with unusual speed and significant new spending. It also finds an unresolved gap at the center of that response: most operators believe they can detect a cyberattack within 24 hours, but the tools they describe relying on were not built to do so.

Eighty-seven percent of operators surveyed rate their ability to detect an active OT breach within 24 hours as confident, scoring themselves a 4 or 5 on a 5-point scale. When asked the basis for that confidence, 51 percent point to IT security tools they themselves describe as having limited visibility into OT-specific traffic. Another 27 percent say they would rely on a field operator or technician noticing that something was wrong. Only 16 percent cite continuous OT monitoring as the foundation of their detection posture.

"This is the most consequential blind spot in U.S. energy infrastructure right now," said Sakari Suhonen, CEO of Tosi U.S. "The sector has the budget, the executive attention, and the will to act. What it does not yet have is detection that actually sees OT. After Operation Epic Fury, that distinction is the difference between catching an intrusion in hours and finding out about it from a production outage."

---

**Webinar:** Tosi will review the full survey findings in a live webinar. **Register here**

---

## A market in active response

Fielded in April 2026, six weeks after the February 28 launch of Operation Epic Fury, the survey documents a sector moving with unusual urgency. Other findings include:

- **Cyber risk has been repriced.** Sixty-three percent of operators report higher cyber risk today than before February 28, with 13 percent describing the increase as significant. Leading drivers include expanding IT and OT convergence, state-sponsored targeting of energy infrastructure, and increased reliance on third-party remote access.
- **Emergency spending is in motion.** Ninety-four percent of operators have either approved (59 percent) or are actively reviewing (35 percent) unplanned OT security funding tied to the post Operation Epic Fury environment. Ninety-five percent expect their OT security budgets to grow over the next 12 months, with one in four expecting growth above 20 percent.
- **Operational impact is widespread.** Ninety-nine of 100 operators report at least one cyber incident category since February 28. Ransomware affecting OT-connected systems and precautionary OT shutdowns triggered by IT-side incidents each affected 48 percent of operators.
- **Detection leads the capability priorities.** Asked to name the single most important OT security capability to acquire or improve in the next 12 months, 22 percent of operators cited continuous monitoring and anomaly detection and 20 percent cited OT-specific incident detection and response. With asset discovery (15 percent) and OT-specific secure remote access (14 percent), detection, visibility, and modern remote access account for 71 percent of named priorities.
- **The largest barrier is human, not financial.** Forty-five percent of operators identify the IT and OT culture gap, where IT security teams lack OT expertise, as the single biggest organizational barrier to faster progress. Operational risk aversion is second at 28 percent. Only 11 percent cite budget, a meaningful shift from prior industry research where budget consistently led.

**Why the gap matters now**

Operation Epic Fury, the February 28, 2026 U.S. and Israeli campaign against Iran, has been followed by sustained Iranian-aligned cyber activity targeting Western critical infrastructure. On April 7, six federal agencies including CISA, the FBI, and the Department of Energy issued a joint advisory (AA26-097A) confirming that Iranian-affiliated actors are actively disrupting programmable logic controllers across US energy, water, and government sectors, with confirmed operational disruption and financial loss. The Railroad Commission of Texas issued a parallel notice to operators on April 10. The Tosi research is the first independent dataset to quantify how the sector itself is responding.

“The next twelve months will see oil and gas spend more on OT security than in the previous several years combined,” Suhonen added. “That spend will land in one of two places. It will close the detection gap with OT-native monitoring, asset visibility, and purpose-built secure remote access. Or

it will deepen the IT-tool stack that operators have already told us cannot see what they need it to see. The data is unambiguous about which path the market needs to take."

**About the research**

The 2026 Oil and Gas OT Decision Maker Survey was independently conducted on behalf of Tosi in April 2026. The sample comprises 100 OT decision makers at U.S. upstream and midstream oil and gas operators ranging from single-site producers to enterprises operating 500 or more sites.

Reporters and analysts can register for the live findings' webinar.

**About Tosi**

Tosi (formerly Tosibox) is a global pioneer in cyber physical systems platforms for operational technology networks. Since 2011, the company has connected, visualized, and secured hundreds of thousands of industrial devices for critical infrastructure operators worldwide. Tosi serves approximately 1,000 direct customers and reaches thousands more through a network of 100+ partners. Tosi is headquartered in Irving, Texas and Oulu, Finland. More at Tosi.net.

**Media Contact:**

Agata Radlak
E-mail: pr@tosi.net

###