tosi

THE DETECTION CONFIDENCE GAP IN US OIL AND GAS OT

Findings from the 2026 Oil and Gas OT Decision Maker Survey

Why 87% of operators believe they can detect an OT breach in 24 hours, why most of that confidence rests on tools that were not built for OT, and what changes in the next budget cycle.

---

100 OT decision makers at US upstream and midstream operators
Independent research conducted by Dimensional Research on behalf of Tosi
Fielded April 2026 | Published May 2026

EXECUTIVE SUMMARY

In April 2026 Tosi commissioned Dimensional Research, an independent research firm, to survey 100 OT decision makers at US upstream and midstream oil and gas operators on the state of OT cybersecurity following Operation Epic Fury. The 18 question survey covered risk posture, incident experience, detection capability, organizational barriers, regulatory exposure, staffing, outsourcing, budget movement, and forward priorities.

The findings describe an industry that is moving capital aggressively. The data also exposes a clear confidence gap. Five themes carry the report.

1. 87% of operators are confident they would detect an active OT breach within 24 hours, but only 16% base that confidence on continuous OT monitoring. Most anchor it to IT tools they describe in the same survey as having limited OT visibility, or to an operator noticing something wrong.
2. 99 of 100 operators report at least one cyber incident category since February 28, 2026. The two most common (precautionary OT shutdowns triggered by IT-side incidents and ransomware affecting OT-connected systems) each touched 48% of the sample.
3. The dominant organizational barrier to faster progress is the IT and OT culture gap at 45%. Operational risk aversion follows at 28%. Only 11% name budget. Three quarters of the barrier landscape is human.
4. 95% of operators expect OT security budgets to grow in the next 12 months and 94% are already moving emergency or unplanned funding through their organizations in response to the post Operation Epic Fury environment. This is current spend, not a future cycle.
5. Detection and asset visibility lead the named priority list for the next 12 months. Continuous monitoring and OT-specific incident detection together account for 42% of operators' single most important capability needs.

Read together, these findings point to a specific decision for OT and security leaders this budget cycle. The capital is moving. The question is whether it goes into more of what the survey shows is not working (IT-centric tools and human watchfulness across a sprawling site footprint) or into OT-native capability that closes the detection gap the data exposes.

ABOUT THIS RESEARCH

Dimensional Research, an independent third-party research firm, fielded the survey in April 2026. The sample comprises 100 OT decision makers at US upstream and midstream oil and gas operators (36% upstream, 64% midstream).

Sample profile

- Respondents include OT security leaders, engineering leaders, and operations technology leaders with direct responsibility for OT cyber programs.
- Operator size ranges from single-site producers to enterprises operating 500 or more sites. 61% operate 100 or more OT sites; 10% operate 500 or more.
- Respondents were screened for direct OT cyber program responsibility and US-based operator employment.

Instrument

The survey ran 18 questions across six topic areas: risk perception and incident experience, remote access and monitoring posture, detection capability, organizational barriers, regulatory exposure and compliance, and forward priorities including staffing, outsourcing, and budget. Two questions used five-point Likert scales and one used forced ranking. The remainder used single or multi-select formats.

Reading the report

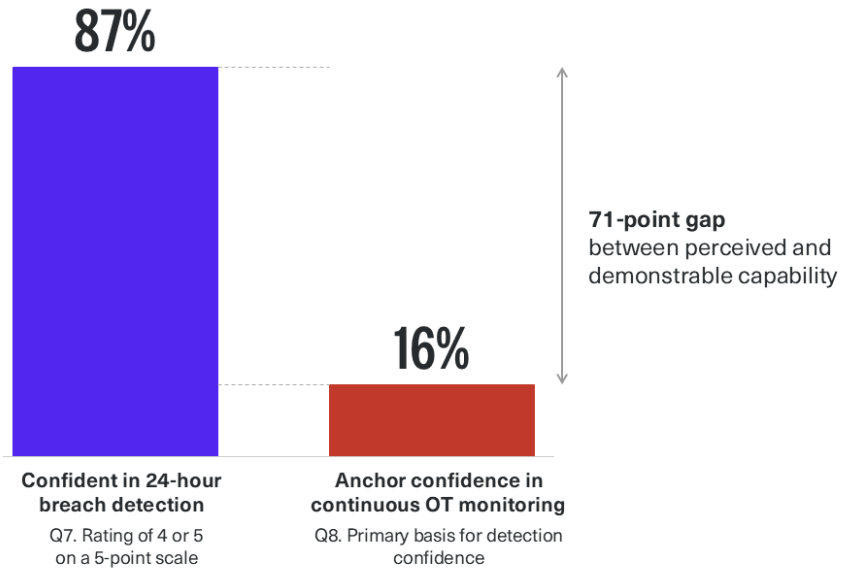
Percentages are rounded to the nearest whole number. Multi-select totals exceed 100% by design. Where bases differ from 100 they are shown inline. Two minor data integrity items are noted in the methodology section.

FINDING 1. THE DETECTION CONFIDENCE GAP

87% of operators rate themselves confident they would detect an active OT breach within 24 hours. Only 16% anchor that confidence to continuous OT monitoring. Most anchor it to IT tools that, in the same survey, they describe as having limited OT visibility, or to a human operator noticing something is wrong.

The Detection Confidence Gap

Self-reported detection confidence vs. the share of operators with continuous OT monitoring as their basis.



Source: 2026 Oil and Gas OT Decision Maker Survey. Dimensional Research on behalf of Tosi, April 2026. n=99 for Q7, n=100 for Q8.

> *"The fallout from Operation Epic Fury has exposed a massive confidence gap in the oil and gas sector. 87% of operators believe they can detect a breach in 24 hours, yet only 16% have the OT-native monitoring required actually to do it. This overconfidence stems from a reliance on IT-centric tools that are blind to the industrial protocols and physical process anomalies of a sophisticated attack."*
>
> **Damon Small** | Board of Directors, Xcape, Inc.

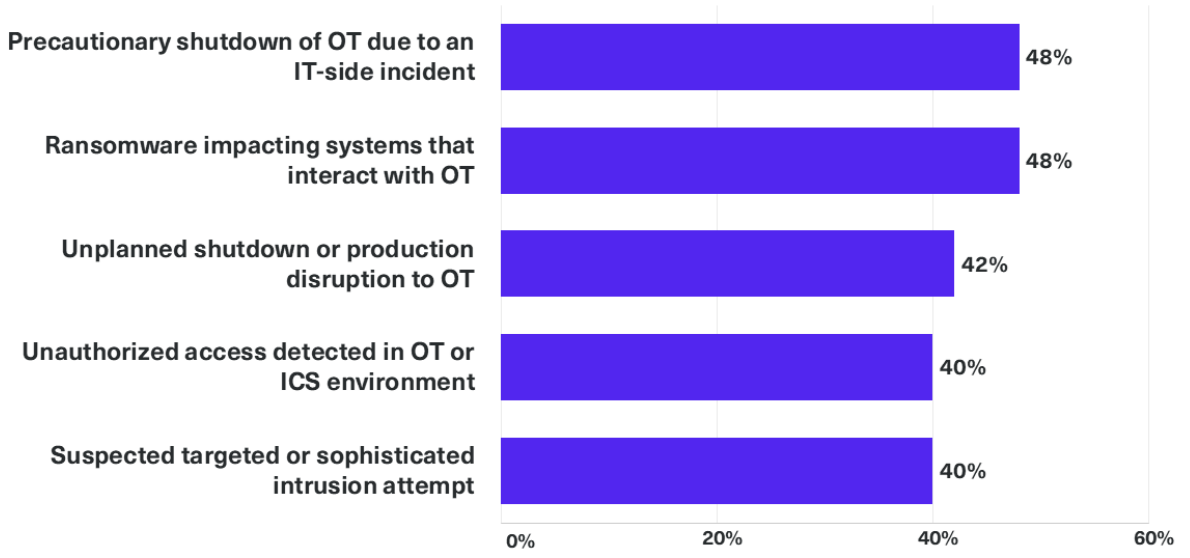
Behind the gap sits a structural reality: only 19% of operators have continuous OT monitoring deployed across 75% or more of their sites. A targeted intrusion that avoids tripping IT-side signatures can move quietly inside that gap.

FINDING 2. THE POST OPERATION EPIC FURY THREAT ENVIRONMENT IS UNIVERSAL

Cyber incidents in the post Operation Epic Fury window are not a tail risk. 99 of 100 operators report at least one incident category since February 28, 2026. 63% rate their current cyber risk higher than before.

Cyber Incidents are Universal in the Post Operation Epic Fury Window

Percentage of operators reporting each incident category since February 28, 2026 (multi-select, n=100).



Q3. Multi-select. Base: 100. Source: 2026 Oil and Gas OT Decision Maker Survey, Dimensional Research on behalf of Tosi, April 2026.

Where the incidents are happening

The two most common incident categories (precautionary OT shutdowns triggered by an IT-side incident, and ransomware on systems that interact with OT) each touched 48% of operators. Among operators reporting higher risk, IT and OT convergence is the leading driver at 49%, ahead of state-sponsored targeting at 37%.

The wider threat picture

April 2026 was the highest-volume ransomware month since BlackFog began tracking in 2020. Dragos tracked 119 ransomware groups targeting industrial organizations in 2025, up 49% year over year, affecting 3,300 organizations globally. Dragos has also documented VOLTZITE, a state-aligned threat group, compromising Sierra Wireless cellular gateways to reach US midstream pipeline operations and pivoting to engineering workstations to extract configuration files. These adversaries do not announce themselves with visible production disruption.

FINDING 3. THE DOMINANT BARRIER IS HUMAN, NOT FINANCIAL

Asked to name the single biggest organizational barrier to faster OT security progress, 45% of operators point to the IT and OT culture gap. 28% point to operational risk aversion: the concern that security tooling will disrupt production. Only 11% cite budget.

Q9. Single biggest organizational barrier to faster OT security progress

Response	Count (%)
IT and OT culture gap: IT security teams lack OT expertise	45 (45%)
Operational risk aversion: fear that security tools will disrupt production	28 (28%)
Budget: security investment competes with operational capex	11 (11%)
Staffing: not enough qualified OT security personnel	9 (9%)
Visibility: incomplete asset inventory	6 (6%)

Base: 99 (one non-response)

A meaningful shift in OT security research

Industry studies have increasingly pointed away from budget as the primary constraint and toward people, governance, and culture. The Tosi findings sharpen that picture for oil and gas: budget falls to fourth place behind culture, operational risk, and staffing combined. Operators are not waiting for funding. They are working through organizational friction that funding alone will not resolve. Tooling decisions that ignore which team owns the deployment, and how the deployment behaves around live operations, will run into the same friction the data describes.

FINDING 4. THE NEXT 12 MONTHS OF SPEND ARE ALREADY MOVING

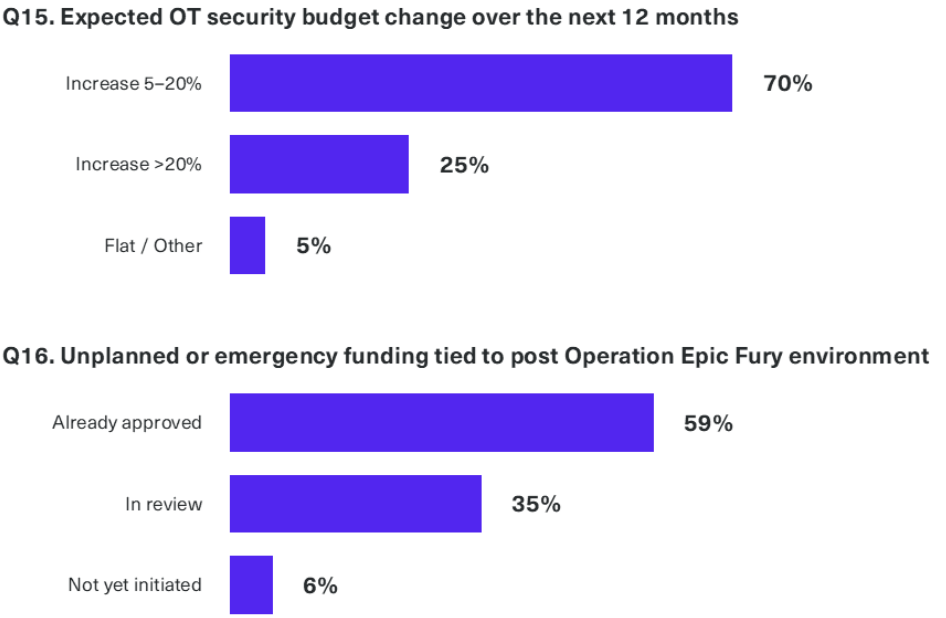
95% of operators expect OT security budgets to grow over the next 12 months. A quarter expect growth above 20%. No respondent reported flat or declining budgets without qualification. More importantly for vendors and partners, 94% of operators are already moving emergency or unplanned funding through their organizations in response to the post Operation Epic Fury environment.

The window is short

This is current spend, not a future budget cycle. Operators are approving funding now, in the next 8 to 12 weeks of decisions. The question is not whether the sector will invest. It is what the sector will invest in.

Budget Movement is Current, Not Future

95% expect 12-month budget growth; 94% are already moving emergency funding (n=100 / n=99).



Q15 base: 100. Q16 base: 99 (one non-response). Source: 2026 Oil and Gas OT Decision Maker Survey, Dimensional Research on behalf of Tosi, April 2026.

> *"The capital is available. What separates operators who get resilience from those who only get activity is whether the investments integrate into operations or just copy IT security models into OT. Operators finally have the tools to do something about OT cyber risk. The question is whether the spend reaches them."*

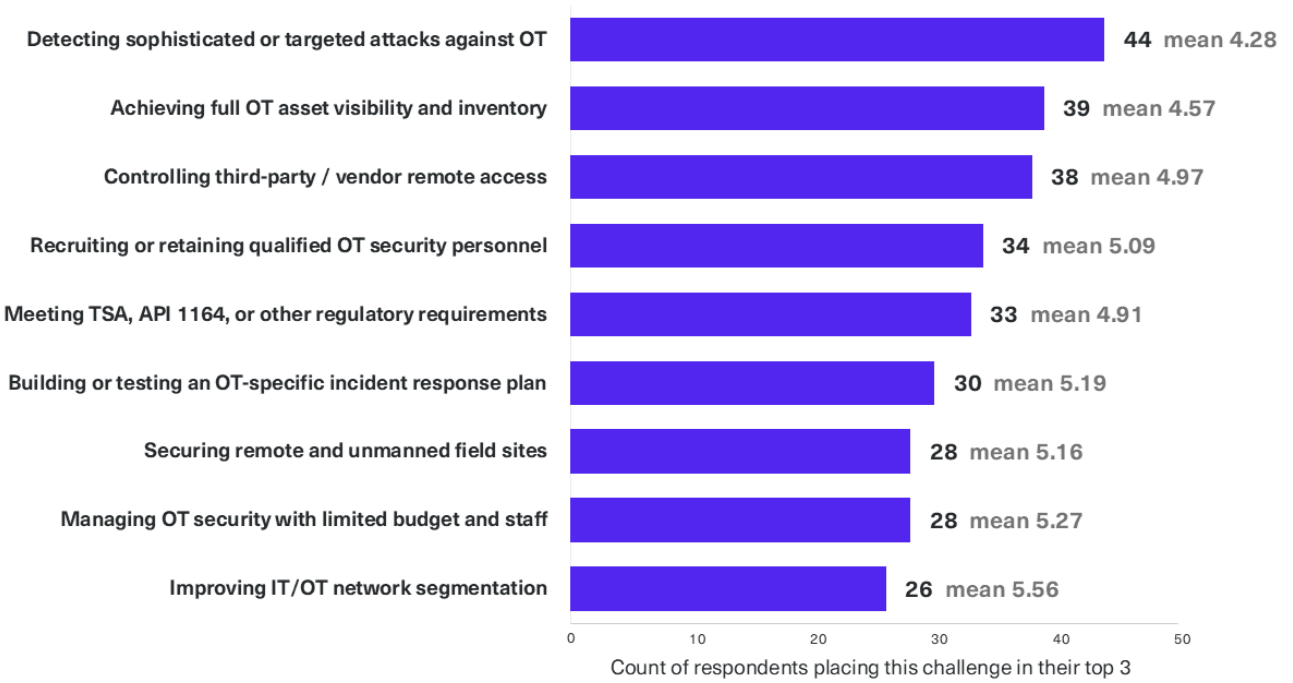
Al Lindseth | Founder, CI5O Advisory Services

FINDING 5. DETECTION AND VISIBILITY LEAD THE NAMED PRIORITY LIST

When operators were asked to name the single most important OT security capability they need to acquire or significantly improve over the next 12 months, detection-related capabilities led at 42% combined. Asset discovery and secure remote access followed. Together, detection, visibility, and modern remote access account for 71% of named priorities. The market is telling itself what to buy next. The risk is that the spend goes back into the same IT-centric tooling the survey shows operators are over-relying on.

Detection and Visibility Lead the Priority List

Q17. Most pressing OT security challenges, forced rank (n=100). Mean rank shown alongside (lower = more pressing).



Q17. Forced rank. Base: 100. Source: 2026 Oil and Gas OT Decision Maker Survey, Dimensional Research on behalf of Tosi, April 2026.

WHAT THIS MEANS FOR THE NEXT BUDGET CYCLE

Every operator should ask four questions before the next investment decision. These are not vendor questions. They are questions an OT or security leader can take into the next steering committee.

1. Is this tool purpose-built for OT environments?

Across the sector only 19% of operators clear 75% site coverage with continuous OT monitoring. The question is upstream of coverage: tools that were not built for OT cannot deliver OT detection at any coverage level. If the answer involves IT-side tooling or relies on a field operator noticing, the position aligns with 78% of the sector. That is the position the data argues against.

2. Can we deploy this tool without interfering with production?

28% of operators name operational risk aversion as the barrier to faster OT security progress. The right question is not whether a tool is technically capable. It is whether the operations team will let it run in production. Deployment behavior, change management, and impact on live processes matter more than feature lists.

3. Can our existing OT security team operate what we are buying?

85% of operators run with five or fewer dedicated OT security staff. Tools that require a team to operate them will not be operated. The realistic acquisition is capability that fits the team that exists, supported by partners that 89% of the sector already engages.

4. Who owns the OT security program when IT and operations disagree?

45% of operators name the IT and OT culture gap as the single biggest barrier to progress. Programs that have not resolved decision rights between teams will move at the speed of that disagreement, not the speed of the funding.

A NOTE FROM TOSI

> Tosi commissioned this research because the conversation we have with oil and gas operators every week has been pulling toward the same set of questions: how to gain visibility across hundreds of sites, how to give vendors and field teams remote access without opening the OT environment to the internet, and how to do all of it with the small teams that the sector actually runs.
>
> We did not write the survey instrument to favor our product. Dimensional Research fielded the survey independently. The findings are presented in their full form so that operators, partners, analysts, and the trade press can read the data on its own terms.
>
> Our reading is straightforward. The detection confidence gap is real, the spend is moving now, and the barrier that decides whether the spend produces resilience is organizational. Tooling that ignores either the OT environment or the lean teams that operate it will not close the gap. Tooling that fits both will.
>
> Tosi builds purpose-built OT security. We have been doing this since 2011, when most of the industry was still treating OT as a subset of IT. We work with oil and gas operators, EPCs, OEMs, and managed service partners to deploy secure remote access and OT network security at field sites in minutes rather than weeks, with operations teams in the driver's seat. If the questions in this paper are the questions your team is working through, we are glad to share what we have learned.

CONTINUE THE CONVERSATION

To request the full data tables, schedule a research briefing for your team, or discuss what an OT-native remote access and monitoring deployment looks like at your sites, contact your Tosi account team or visit **tosi.net**.

METHODOLOGY

Research firm and field

The 2026 Oil and Gas OT Decision Maker Survey was fielded by Dimensional Research, an independent third-party research firm, in April 2026. The sample comprises 100 OT decision makers at US upstream and midstream oil and gas operators (36% upstream, 64% midstream).

Respondent profile

Respondents include OT security leaders, engineering leaders, and operations technology leaders with direct responsibility for OT cyber programs. Respondents were screened for direct OT cyber program responsibility and US-based operator employment. Operator size ranges from single-site producers to enterprises operating 500 or more sites; 61% of respondents operate 100 or more OT sites.

Instrument

The instrument comprised 18 questions across six topic areas: risk perception and incident experience, remote access and monitoring posture, detection capability and confidence, organizational barriers, regulatory exposure and compliance, and forward priorities including staffing, outsourcing, and budget. Two questions used five-point Likert scales. One question used forced ranking. The remainder used single or multi-select formats. Percentages are rounded to the nearest whole number. Multi-select totals exceed 100% by design. Bases that differ from 100 are noted inline.

Notes on the data

1. Q11 (compliance posture against TSA Pipeline Security Directives) was a routed question, asked only of respondents who indicated their organization is subject to those directives in Q10. The 33 responses are TSA-regulated operators only and should be read as a sub-sample rather than a survey-wide finding.
2. Self-reported confidence questions, including Q7 (24-hour detection confidence) and Q12 (compliance driving genuine improvement), are subject to a documented tendency of survey respondents to rate themselves and their organizations more favorably than independent assessment would. The 71-point gap between Q7 detection confidence and Q8 capability basis, and the absence of any "strongly disagree" responses on Q12, are both consistent with this pattern. Readers should treat self-rating data as directional rather than absolute.

Citation

The findings in this paper may be cited externally with attribution to the 2026 Oil and Gas OT Decision Maker Survey, conducted independently by Dimensional Research on behalf of Tosi, April 2026.