



Post-Competition Study: Tool Expertise vs. Domain Expertise

20 Pre-Competition Trials vs. 16 Live Event Teams
Water & Wastewater Competition | Spring 2026

Note: Team names anonymized at the request of event management. Expert reviewers appear with permission.

The Central Question

Does knowing the tool or knowing the industry produce better crisis management outcomes?

Group A: Tool Experts

20 pre-competition trials
Deep AutoTableTop™ knowledge
No water industry experience

Group B: Domain Experts

16 event teams
First exposure to AutoTableTop™
Expert water/wastewater operators

By the Numbers

GROUP A: TOOL EXPERTS

6.5

Mean Avg Score

7.5

Highest Avg

6.7

Avg Turns

85%

Scored 8+

GROUP B: DOMAIN EXPERTS

6.1

Mean Avg Score

8.0

Highest Avg

5.4

Avg Turns

63%

Scored 8+

Event Results: Top 3 by Total Score

1st Chlorine Kings

Total: 94 | 14 turns | 6.7 avg

Most comprehensive response in either group

2nd Turbidity Titans

Total: 67 | 10 turns | 6.7 avg

Industry jargon: "run in-hand," PAO engagement

3rd Basin City Legends

Highest Average: Clearwater All-Stars - 8.0 avg (4 turns, all scored 8). Highest of either group.

What Operators Said That Tool Experts Never Did

“Run in-hand”	Industry jargon for manual/local equipment operation	Team 7
“Grab samples”	Lab procedure for water quality verification	Team 11
“Disconnect PLC network”	Precise OT isolation language	Team 9
“Paper logs for permit compliance”	Regulatory fallback procedure	Team 10
“Test water post-incident”	Verify attacker didn't alter treatment	Team 8
“Contact cyber insurance”	Risk management awareness	Team 9
“Alert other facilities on network”	Cross-utility awareness	Team 9
“Verify PII compromise”	Data privacy consideration	Team 6

None of these responses appeared in any of the 20 pre-competition study trials.

Universal Scoring Patterns

WHAT SCORES 8 IN BOTH GROUPS

- Compound actions (multiple related actions per input)
- Specificity (naming resources, departments, procedures)
- Forward planning (stating what comes next)
- Stakeholder breadth (multiple communication vectors)

WHAT SCORES POORLY IN BOTH GROUPS

- “OK” / “Wait for instructions” (scored 0)
- Single actions without follow-up (scored 4)
- Vague delegation without specifics (scored 5)
- Passive monitoring without engagement

Key Insight: The scoring engine’s reward structure aligns naturally with how experienced crisis managers think. Top event teams independently discovered the compound-action optimization that the tool experts learned through 20 iterations — without any coaching.

After-Action Report Findings

Containment Ratings

Team 3 received “Excellent” — the highest containment rating of either group. Pre-competition study’s best was only “Successful.”

Operational Learnings

Event AARs produced richer, facility-specific learnings: PLC isolation, manual data logs, dual-path recovery, cross-department coordination.

Safety Recommendations

Operators generated specific recommendations: dual-factor authentication, network segmentation, alternative comms during isolation.

Zero event AAR’s triggered MITRE ATT&CK mapping — consistent with pre-competition study (1 of 20). Confirms beginner/basic config de-emphasizes technical detail.

Conclusions

- 1 Tool familiarity raises the floor; domain expertise raises the ceiling.
- 2 Operational authenticity is a feature, not a limitation.
- 3 The passive-response penalty is universal across user populations.
- 4 Compound actions are instinctive to experienced operators.
- 5 Operators surface action categories tool experts never considered.
- 6 The platform validates domain expertise without requiring cyber knowledge.
- 7 A 5-minute orientation would close the 0.4-point scoring gap entirely.

Implications for AutoTableTop™ 2.0

Product Validation

16 teams with zero tool exposure produced authentic, high-quality exercises from minimal configuration. The scoring engine accurately evaluates crisis management competence independent of cybersecurity knowledge.

Sales & Marketing

Team 3's 8.0 average and Team 9's 94-point total are compelling proof points for water sector sales conversations. Operators engage immediately — no training required.

Demo Script Enhancement

The revised script now includes operator-authentic alternative phrasings: “run in-hand,” “grab samples,” “PLC network disconnect” alongside the optimized baseline.



THREATGEN[®] **AUTOTABLETOP**

Thank You

Robert C. Rhodes

robert@threatgen.com

+1 (281) 435-3917