

# Beyond the Headlines: Building Operations That Hold Under Pressure

The real question in OT security is not what the next attack looks like. It is whether your operations can continue safely when disruption arrives — and whether you are solving that problem alone or with a community that has already seen it.

OT-ISAC Community | TLP:WHITE

*OT operators across the Asia-Pacific region are not struggling because vulnerabilities exist. They are struggling because operational decisions are being made with incomplete context — every day, at every site, across every sector. The organisations responding best are not always the ones with the largest security budgets. They are the ones investing in visibility, operational coordination, and trusted intelligence exchange.*

## SETTING THE FRAME

### The conversation is shifting — and it should

Cybersecurity conversations in OT environments have historically been dominated by threat narratives: ransomware, nation-state actors, catastrophic scenarios. Those concerns are real and worth understanding. But for operators responsible for keeping critical systems running, the more useful question has never been "what is the next big attack?" It is: how do we build operations that remain reliable even when disruption happens?

That shift — from threat-centric to resilience-centric thinking — is what the OT community is increasingly asking for. And the incidents making headlines over the past 12–18 months, read carefully, support exactly that framing.

#### OLD QUESTION

*"How do we stop every threat?"  
"How do we block the next attack?"  
"How many vulnerabilities did we patch?"*

#### MORE USEFUL QUESTION

*"How do we sustain safe operations despite uncertainty?"  
"What is our minimum viable operational state?"  
"Are we reducing decision uncertainty for our operators?"*

## WHAT THE INCIDENTS ARE SIGNALLING

### Patterns from documented global incidents — read for operational lessons, not alarm

The following patterns are drawn from publicly documented incidents and widely cited research. Confidence levels reflect what the evidence actually supports — not worst-case extrapolation.

#### Internet-exposed OT assets remain a consistent entry point

Across multiple documented incidents — including the December 2025 Poland energy sector compromise, attributed with medium confidence to a state-affiliated actor — initial access came through vulnerable internet-facing edge devices, not sophisticated zero-days. Remote access gateways, engineering workstations, and vendor connectivity pathways are recurring vectors in published post-incident analysis. The operational lesson: unmonitored trust boundaries, not novel malware, are where most documented intrusions begin.

Confidence: high – multiple corroborating incidents

#### Recovery is harder than most continuity plans assume

Research on manufacturing ransomware recovery — as well as post-incident reporting from energy and utilities sectors — consistently highlights that restoring servers does not restore operations. Organisations encounter challenges with OT reconnection, supplier coordination, trusted recovery sequencing, and safe degraded operations. The gap between IT recovery and OT operational continuity is well-documented and often underestimated in advance planning.

Confidence: high — consistent across published post-incident reviews

### Industrial environments account for a significant share of ransomware activity

Multiple research sources tracking ransomware incidents place industrial organisations — manufacturing, energy, utilities, transport — among the most frequently reported sectors. Figures vary by methodology: some reports place industrial sector exposure at roughly 25–30% of observed ransomware activity. These numbers should be read directionally, not as precise measurements, given underreporting across the sector.

Confidence: medium — sector share estimates vary across sources

### Sophisticated intrusion paths increasingly use legitimate tools

Published threat intelligence from Dragos, CISA, and others documents a pattern of adversaries leveraging legitimate remote access mechanisms, engineering software, and vendor credentials rather than custom malware. This creates detection challenges in environments where the same tools are used operationally every day. Detection strategies built around malware signatures alone are insufficient for this pattern.

Confidence: high — corroborated across multiple vendor and government sources

### APAC operators face targeted exposure, not just spillover

Publicly available threat intelligence identifies active campaigns targeting operators across Asia-Pacific — particularly in energy, maritime, telecommunications, and manufacturing sectors — linked to geopolitical dynamics including South China Sea tensions. Named threat groups including SYLVANITE (Philippines-linked targeting documented by Dragos 2026) and AZURITE (active across APAC, with noted overlaps with Flax Typhoon) represent documented, not hypothetical, regional exposure. Attribution confidence varies; these findings should be treated as intelligence inputs, not definitive conclusions.

Confidence: medium — based on vendor threat intelligence; independent confirmation varies by actor

*The most important observation across these incidents is not the sophistication of the attacks. It is what they reveal about operational blind spots — delayed detection, fragmented ownership, incomplete asset visibility, and the absence of peer context when decisions needed to be made.*

## THE THREE QUESTIONS OPERATORS FACE DAILY

Not theoretical. These surface in every engagement, every after-action, every peer conversation.

#### Question 01

*"Do we actually know what is exposed today — not last quarter, not from the last audit. Today."*

Many operators continue to manage asset inventories that are incomplete, outdated, or limited to IT-visible assets. Engineering workstations, legacy serial-to-IP devices, expanded vendor connectivity, and forgotten remote access pathways regularly appear in assessments as gaps. The risk is not simply "exposure." The operational risk is uncertainty — because uncertainty slows decisions, and delayed decisions are where operational consequences compound.

**STRATEGIC REFRAME** The goal is not more dashboards. It is reducing uncertainty for the operators making calls under pressure. Even partial, well-curated visibility improves prioritisation more than comprehensive but unactionable data.

#### Question 02

*"If disruption happens tomorrow, what can still safely operate?"*

This is where cybersecurity and operational engineering converge — and where many organisations discover their continuity planning has gaps. Recovery plans are often written around technology restoration. But OT environments require something more: safe minimum operations, trusted reconnection sequencing, and the ability to sustain degraded-but-safe states while full restoration is underway. Engineering disciplines — HAZOP, LOPA, redundancy planning, fail-safe design — already provide the mental model. Cyber resilience planning should be built on the same foundation.

**STRATEGIC REFRAME** The objective is not perfect recovery. It is graceful degradation — the ability to identify, in advance, what the organisation can safely sustain, and under what conditions it can safely reconnect.

#### Question 03

*"Are we solving the same problems that peers have already worked through — alone?"*

Across the region, operators encounter similar exposed technologies, comparable vendor relationships, shared network architectures, and recurring operational dilemmas. Yet investigations still largely happen in isolation. One organisation spends days validating a risk that a peer may have assessed weeks earlier. The duplicated effort is real and measurable — and in resource-constrained OT teams, it is not a minor inefficiency. It is a structural disadvantage.

**STRATEGIC REFRAME** Collective intelligence is not about sharing sensitive infrastructure data. It is about reducing duplicated uncertainty across the community — accelerating validation, improving prioritisation, and helping operators focus limited resources on what actually matters.

#### WHAT CHANGES WITH COLLECTIVE INTELLIGENCE

### The compounding value of operating with the community

Collective intelligence — done well — is not a reporting exercise. It is a structural advantage. What one operator learns from an incident, the community can act on before that pattern reaches the next site. What one team cannot generate alone in terms of context and peer validation, the network provides. The outcome is not just awareness. It is operational resilience that compounds across organisations.

*"The strongest OT organisations in the coming years will not necessarily be the ones with the largest security stacks. They will be the ones that learn faster, collaborate better, and reduce operational uncertainty across their teams."*

// Shared baseline

#### Shared baseline, not shared secrets

Anonymised signals across member environments help operators distinguish genuinely anomalous activity from what peers are also experiencing — without exposing sensitive infrastructure details.

// Early signal

#### Early signal before it becomes an incident

When a member surfaces an early indicator, that signal — anonymised and enriched — circulates to relevant members. One site's early-stage observation becomes the community's pre-incident intelligence.

// Prioritisation

#### Operational prioritisation, not raw CVE lists

OT-ISAC advisories use SSVC framing — factoring in exploitation evidence, sector exposure, and operational constraints. Context replaces score-based guesswork.

// Peer validation

#### Peer validation without competitive risk

Community sessions give operators a venue to validate concerns with peers — practitioner-to-practitioner, vendor-neutral, without legal exposure. The knowledge stays in the room.

// Reciprocity

#### Signal reciprocity — contribution compounds

What a member contributes returns as enriched, community-validated intelligence. A weak signal in, a confirmed pattern out. The more the community shares, the higher the return.

// Coverage

#### Coverage that scales with resource constraints

With only 19% of organisations considering their OT security teams fully skilled (SANS, 2025), collective coverage compensates structurally for what individual teams cannot sustain alone.

## Five ways community membership becomes operational capability

OT-ISAC does not replace security consultants, vendor tools, or internal teams. It provides what individual organisations structurally cannot generate alone: community-validated context, peer intelligence exchange, and operationally grounded prioritisation across sectors and geographies.

- 01 Shared baselines across sectors.** Aggregated, anonymised signals from member environments support sector-specific baselines. What looks anomalous at one site can be validated — or escalated — against what the broader community is experiencing. This directly addresses the uncertainty in Question 01.
- 02 Early warning circulation before incidents propagate.** Indicators surfaced by members — anonymised and enriched — are redistributed to relevant operators. One organisation's early-stage observation becomes the community's pre-incident intelligence. This directly addresses Question 02.
- 03 SSVC-framed advisories — operational context, not raw scores.** Prioritisation reflects actual adversary behaviour in your sector, your region, and your operational constraints — not a spreadsheet of CVSS numbers sorted high to low. This directly addresses the prioritisation gap in Question 03.
- 04 Practitioner-to-practitioner community sessions.** Geography-specific, sector-specific, vendor-neutral. Operators share what they are actually seeing — not curated for a product pitch. The format is designed for the questions teams are genuinely reluctant to raise with vendors or regulators.
- 05 Resilience-focused exercises and tabletop frameworks.** Moving beyond detection drills toward operational continuity — safe minimum operations, degraded-state decision pathways, and OT-aware recovery sequencing. Designed with the engineering discipline OT environments require.

### A FINAL REFLECTION

In OT environments, eliminating all risk has never been realistic. What matters is the ability to sustain safe and reliable operations — even under uncertainty, during disruption, and when the full situation is still unfolding.

That capability is not built through fear-driven investment cycles or reactive compliance exercises. It develops over time through stronger visibility, engineering discipline, operational coordination, and trusted communities willing to share lessons learned.

Resilience is rarely built in isolation. OT ecosystems are deeply interconnected — supply chains overlap, vendors are shared across industries, operational technologies span multiple sectors, and disruption at one site can create downstream effects across the wider ecosystem.

**The organisations that will be best positioned in the years ahead may not necessarily be the ones with the most technology. They will be the ones that reduce uncertainty faster, adapt operationally faster, and learn collectively faster.**

### Resilience is a community outcome, not an individual one

OT-ISAC connects operators across energy, water, manufacturing, and critical infrastructure in Asia-Pacific. The intelligence your team cannot generate alone is already circulating in the community — the question is whether you are part of the loop.

Connect with us and be part of the community: [info@otisac.org](mailto:info@otisac.org) | [otisac.org](https://otisac.org)

Incident references: CISA Alert AA26-041A (Poland Energy Sector, Feb 2026) · Dragos 2026 OT/ICS Year in Review · SANS ICS Security Survey 2025 · Cyble Annual Threat Landscape Report 2025 · CYFIRMA Philippines Threat Landscape 2025-2026 · Forescout Vedere Labs ICS Vulnerability Report 2026.

Confidence levels reflect publicly available corroborating evidence at time of publication. Named threat actor attributions are drawn from vendor threat intelligence and should be treated as analytical assessments, not definitive conclusions.

TLP:WHITE — may be shared without restriction. For member-classified intelligence, contact OT-ISAC directly. Copyright 2026 GRF Asia Pacific Pte Ltd. All rights reserved.