Building Collective OT Cyber Resilience Across Critical Infrastructure

OT-ISAC COMMUNITY IMPACT REPORT

OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OUR MISSION

Operational Technology Information Sharing and Analysis Center (OT-ISAC) facilitates sharing of tactical and strategic security details, providing early insight into emerging threats, detection techniques and containment measures.

Exchanged information includes vulnerabilities and attacks to OT systems and relevant IT applications affiliated with OT systems.

Survey of OT-ISAC Members

Member feedback demonstrates strong confidence in OT-ISAC's value as an OT/ICS-focused community, clearly differentiated from generic cybersecurity information sources. Across Energy, Utilities, Water, Oil & Gas, Maritime, Healthcare, Manufacturing, and Government, members consistently highlight the importance of actionable OT-specific intelligence, practitioner-led engagement, and trusted peer collaboration.

The majority of respondents rate their likelihood to recommend OT-ISAC between 8 and 10, reflecting strong advocacy and trust.

Members highlight OT-ISAC's neutral stance, the practical framing of shared intelligence, and the opportunity for cross-sector learning within the community.

Constructive feedback also provides clear direction for continued impact: to deepen OT/ICS specificity, reduce overlap with IT-centric cyber reporting, and expand actionable guidance and hands-on capability building aligned with OT resilience goals.

Overall, the member survey reflects OT-ISAC's role in underpinning operationally relevant collaboration within the OT cybersecurity ecosystem.

Five Core Benefit Pillars of OT-ISAC

From Shared Insights to Operational Action

Pillar 1: Community-Amplified OT/ICS Intelligence

Risk Awareness & Prioritization.

OT-ISAC brings together trusted inputs from members, public advisories, partners, and sector-specific sources, and contextualizes them for OT/ICS environments.

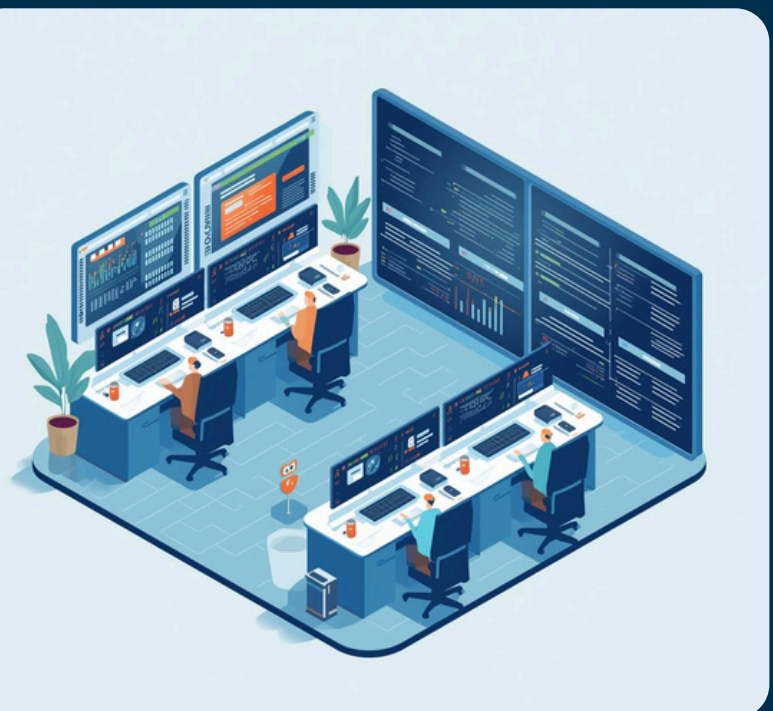
The focus is on collective situational awareness, not replacing internal security teams or commercial tools.

Members value intelligence that includes OT-relevant CVEs, IOCs, hashes, IPs, and adversary techniques, framed with sector and geographic context to support prioritisation.

Proof of value

- Reduced noise from non-applicable cyber reporting
- Faster understanding of which threats matter operationally
- Stronger peer-informed risk prioritisation

"OT-ISAC provides timely information on OT threats so that alerts can be flagged early and mitigating measures initiated promptly."
– Water Utility Member



Pillar 2 — OT-Focused Incident Analysis & Response

Readiness & Decision Confidence

Members rely on incident and ransomware analysis framed through OT impact, including safety, availability, and physical process considerations. OT-ISAC supports understanding of how incidents unfold in industrial environments and what response actions are feasible under operational constraints.

This pillar strengthens cross-functional readiness, improving coordination between OT, IT, engineering, safety, and management teams.

Proof of value

- Clearer response decision-making
- Supports more informed and coordinated OT incident response decision-making.
- Improved coordination across functions

"OT-ISAC has been invaluable to our company, providing high-quality threat intelligence and enriching learning sessions."
– Energy Sector Member

Pillar 3 — Vulnerability & Legacy System Risk Management

Risk Reduction Within Operational Constraints

Members consistently highlight challenges related to legacy OT systems, long asset lifecycles, and limited patching windows.

OT-ISAC supports risk-informed decision-making by contextualising vulnerability intelligence and sharing practical mitigation and compensating-control considerations.

The emphasis is on operational feasibility, rather than prescriptive remediation.

Proof of value

- Safer vulnerability prioritisation
- Reduced exposure without disrupting operations
- Improved handling of unpatchable systems

Pillar 4 — Threat Modelling & Defensible OT Architectures

Prevention & Containment

Members have expressed strong interest in OT-specific threat modelling and defensible architecture concepts, including segmentation, zoning, controlled interconnections, and least-privilege communication.

These practices are recognized foundations for reducing cyber risk in industrial environments.

OT-ISAC's role in this area is to facilitate shared understanding, peer learning, and capability development, rather than to act as a delivery or advisory consultancy.

Engagements are structured to support members in building internal readiness, and to complement–rather than replace–formal assurance or consulting activities.

Proof of value

- Improved internal understanding of OT threat modelling
- Greater clarity on high-risk pathways
- Stronger alignment between cybersecurity governance and OT operations

Engagement Objectives

- Co-develop a OT threat model for one representative OT threat scenario
- OT-ISAC worked alongside the member's staff to walk through a single scenario using recognized industry frameworks and best practices, focusing on process and understanding.
- Knowledge and know-how transfer
- OT-ISAC facilitated structured discussions on OT cybersecurity principles and OT threat modelling approaches to build internal capability and confidence.

Pillar 5 — Operational Recovery, BIA & Resilience

Continuity & Long-Term Resilience

Beyond prevention and response, members emphasise recovery readiness.

OT-ISAC supports discussions around OT-specific Business Impact Analysis (BIA), system restoration planning, and dependency mapping for critical processes.

This pillar aligns directly with objectives for service continuity and public confidence.

Proof of value

- Faster, safer recovery
- Improved continuity of essential services
- Stronger organizational resilience

"Yes. OT-ISAC has been helping us in our journey towards OT Cybersecurity for the past 3.5 years. I have attended numerous sessions of threat calls, talks and workshops arranged by OT-ISAC."
– Utility Sector Member

OT-ISAC Most Valued Membership Support

- OT Cyber Threat / Incident Analysis Report
- Cyber Vulnerability Analysis Report
- Weekly Analyst Ransomware Report
- Sector Round-Up Report
- OT-ISAC Observables Collection
- OT TTX Support

Members value these products most when they include OT context, operational implications, and practical next steps.

Expected Impact of OT-ISAC Engagement

Members consistently describe impact in qualitative, operational terms:

- Improved situational awareness of OT threats
- Enhance OT incident response decisions
- Better alignment between OT, IT, engineering, and operations
- Heightened readiness to assess and respond to ransomware and vulnerability risks within OT environments.
- Stronger peer learning and collaboration within OT Community

Member feedback reflects OT-ISAC's role in fostering trusted collaboration and delivering operationally relevant insight across the OT cybersecurity ecosystem. Through sustained community participation and shared learning, OT-ISAC provides a platform where organizations can both contribute to, and benefit from, collective efforts to strengthen OT cybersecurity resilience.

OT-ISAC welcomes critical infrastructure operators and practitioners to engage with the community—sharing experience, learning from peers, and working together to advance resilient and secure OT operations across sectors.

To learn more about the Community, reach out to membership@otisac.org