# A YEAR IN REVIEW

OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OT THREAT LANDSCAPE

COMMUNITY

OT -ISAC CAPABILITIES

# Foreword

Welcome! We appreciate your interest in learning more about the Operational Technology Information Sharing and Analysis Center, a non-profit member community for Critical Information Infrastructure (CII) owners and operators, to share cyber warning and mitigation information for mutual defense.

In this brief, you will learn more about the membership make-up, the features of being a member, the type of information shared, as well as the technology the community uses and how OT-ISAC analysts work with security vendors to provide the most valuable and time-sensitive intelligence for your security team.

And not only does OT-ISAC offer threat information and vulnerability alerts, it includes a Critical Information Notification System to gather stakeholders in the event of a systemic threat to CII. In addition to virtual meetings, OT-ISAC also holds an annual conference for opportunities to network and learn from experts in the OT security field.

Don’t hesitate to reach out with any questions or a sample of the information the community exchanges every day.

# OT Threat Landscape

**Threats to Operational Technology (OT) networks remain high in 2020 as threat actors look to cause disruptions to critical services and industrial processes.**

**Last year, we witnessed an expansion in the OT cyber threat landscape driven by the rise in ransomware attacks targeting industrial organizations and the continued targeting of critical infrastructure by politically motivated threat actors.**

### Rise in Ransomware Attacks

In 2020, OT-ISAC tracked over 450 ransomware incidents that impacted organizations across the aviation, energy, government, healthcare, manufacturing, maritime, transportation and water sectors a majority of these incidents were from the manufacturing sector. We expect this trend to persist in 2021 as ransomware operators evolve their Tactics, Techniques, and Procedures (TTPs), exploiting the latest vulnerabilities (e.g., MS Exchange Server zero-day vulnerabilities released in March 2021) and leveraging high profile clients of suppliers and vendors to make ransom demands more effective (as in the case of Apple supplier Quanta).

Organizations are finding efficiencies in convergence, and as a result, more industrial control systems and devices that were traditionally air-gapped are now exposed to the internet.

What's also exposed to the internet—and attackers—are the vulnerabilities and misconfigurations inherent in these systems. These security flaws aren't easily mitigated given the uptime demands in many industrial settings, making them prime targets for opportunistic—and targeted—attacks such as ransomware or those an advanced attacker might deploy.

As a result, security decision-makers are being forced to reassess their networks' risk posture and risk tolerance. The first, and most logical step, is the need for protocol-specific visibility into industrial assets running on the network, and what processes those assets support. An asset inventory helps a CISO or network manager evaluate and prioritize vulnerability management and security feature updates. The COVID-19 pandemic has also put an emphasis on secure remote access to industrial networks and devices. It's a mandate that operators and engineers be able to monitor and terminate remote sessions if malicious activity triggers an alert; logging is also an imperative for forensic investigations. "

***-Claroty***

## Predictions

*Based on Group-IB's observations of the ransomware threat landscape, our experts have compiled the following list of trends that the world should look out for in the coming year:*

1. Due to how profitable they are, the number of public and private Ransomware-as-a-Service programs will keep growing.

2. Ransomware operators will continue to focus on enterprise networks.

3. More actors will focus on gaining access to enterprise networks for resale purposes.

4. Ransomware-as-a-Service programs will start offering Linux variants more often.

5. Some threat actors may abandon the use of ransomware and instead focus on exfiltrating sensitive data for extortion.

6. More state-sponsored threat actors will be involved in Big Game Hunting, including those who use it for disruptive purposes.

7. Threat actors will start attacking CIS countries more heavily, especially countries with extensive enterprise networks.

8. Growing ransom demands will be accompanied by increasingly advanced techniques.

# OT Threat Landscape

## 9 out of 10

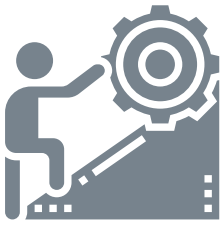
Organizations experienced at least one OT system intrusion in the past.

**Impact:**
Operational outages impacting revenue are a real concern given the dangers inherent in industrial facilities.

*Reference Fortinet's 2020 State of Operational Techonlogy and Cybersecurity Report*

---

## There are several common threads to any kind of attack against critical infrastructure that must be addressed:



First, increased connectivity (convergence) between external networks and formerly isolated Operational Technology networks exposes these sensitive networks to additional risks for which they were not designed.

Second, most operators of critical infrastructure lack a comprehensive inventory of the assets within their estates, and the interconnectivity between these assets. This lack of inventory makes it impossible to get a full understanding of an organization's full risk exposure.

Third, there is a large population of commodity operating systems existing within the OT environment. These are often unsupported, and rarely see patches. With the emergence of increased connectivity to external networks, these unmaintained machines serve as an excellent platform from which to launch a cyber-attack.

In conclusion, organizations need appropriate cyber hygiene in both their OT infrastructure and their Active Directory to reduce their cyber exposure and ensure that attack paths are cut off. These collective efforts can help avoid having to respond to a security crisis that can stop operations and potentially put human lives at risk.

***-Tenable***

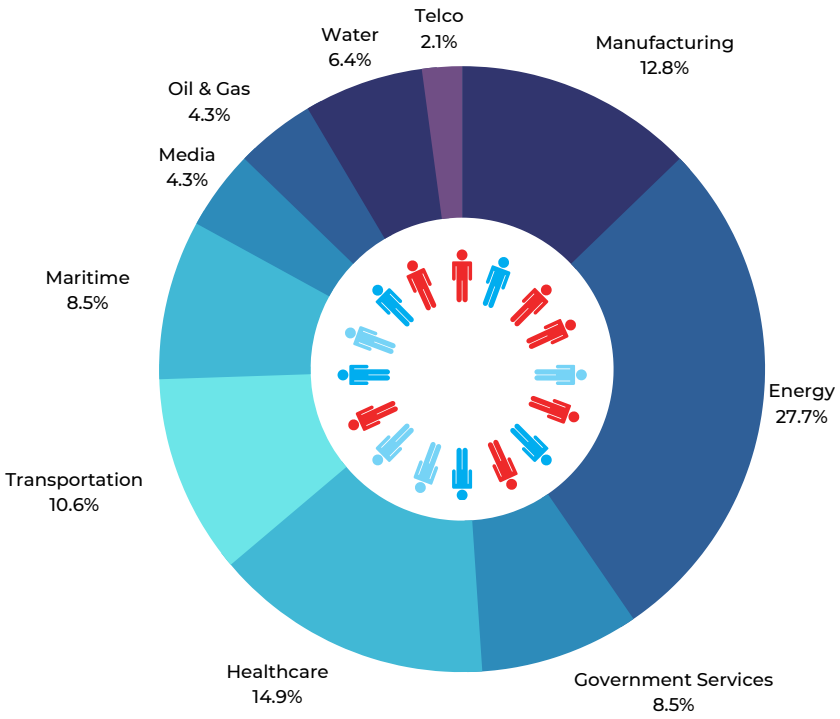
# Community

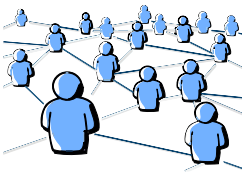
## OUR MISSION

**OT Cybersecurity 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.

### OT-ISAC Members Breakdown



## OUTREACH

*OT-ISAC engage in targeted outreach activities that help members improve overall cyber resiliency of their critical assets and environments.*

**OT-ISAC Monthly Threat Calls**

Our threat calls help members keep up with the latest cyber threat landscape developments impacting industrial organizations and critical services, increasing their overall situational awareness and understanding of the cyber threats and risks to their organizations.

**OT-ISAC Training**

Our trainings boost members' understanding of key OT security concepts and support their efforts to safeguard critical OT assets. Trainings are provided by OT-ISAC and Global Resilience Federation partners.

**Member Meetings, Sector Joint Working Group & Community Events**

Meetings and Community Conferences aim at raising awareness and sharing best practices within OT security.

# Community

## OT-ISAC AREAS OF INFORMATION SHARING

- Threats Advisories
- Vulnerability Reports and Analysis
- Sector Alerts
- Incident Advisories
- Mitigation Measures
- Best Practices & Lessons Learnt
- Real Time Crisis Communications
- Policy Developments Notification
- Monthly Analyst Threat Briefings
- Dark Web Reports (Shared by Partners and Community)

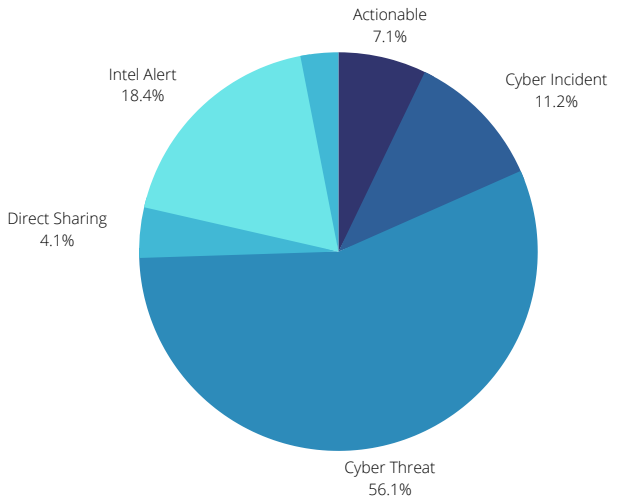



*Illustration shows Alerts shared in the OT-ISAC Portal*

## OT-ISAC SOURCES

### Partners

Trusted partners include sister ISACs/ISAOs, CERTs and commercial vendors

### Members

Member sharings on threats and technical indicators

### OT-ISAC Analysis

Curated list of open/closed source threat events that are relevant to OT-ISAC members

## EMPOWER WITH TOOLS

We empower Members with technology solutions such as our Cyware communications portal and Malware Information Sharing Platform to facilitate the sharing of threat intelligence and secure their assets.

CYWARE

MISP Threat Sharing

## CRITICAL INFORMATION NOTIFICATION SYSTEM (CINS)

The OT-ISAC Critical Information Notifications System contacts members during incidents which could have significant impact on the CII community. Includes notifications via text, phone, and email.

# OT-ISAC Capabilities

**Critical Information Notification System (CINS)**

The OT-ISAC Critical Information Notifications System contacts members during incidents which could have significant impact on the CII community. Includes notifications via text, phone, and email.

**Ability to Send/Receive Requests For Information (RFIs) within the OT-ISAC Community and Trusted Partners**

RFIs allow members to engage local OT-ISAC Analysts and leverage help and advice from a broader network, including other industry sectors which face similar threats to their businesses. RFIs allow access to a wider range of information to support protection and mitigation and to help mitigate successful attacks/intrusions using best practices or known solutions

**OT Threat Modelling**

The goal of this engagement is to kickstart and support our Member's efforts in developing a threat model and vulnerability management programme for its critical OT assets.

**OT-Vulnerability Research**

The vulnerability research initiative aims to help OT-ISAC members identify unknown vulnerabilities that may be present within their OT environment and assets.

**OT-ISAC Monthly Report**

Receive a monthly report with analysis of the key threats, incidents, vulnerabilities and developments impacting CII sectors

**OT-ISAC Community Portal**

Members will obtain and share threats , incident information, vulnerability details, APT activity, IOC etc.

**Receive actionable information that allows your organization to advance resilience by incorporating it in their own defensive architecture to prevent or respond to threats.**

The OT-ISAC portal provides a platform for sharing cyber and physical threat intelligence, in real time.

**Participation in OT-ISAC Member Commitees**

Member Committees and Working Groups are member-driven efforts to improve the community's security posture and enhance capabilities by coordinating response and proposing policies and best practices.

**Community Events**

- Annual Summit Passes (In-Person & Virtual)
- Member Meetings
- Member Briefings

**OT-ISAC Intelligence Monthly Threat Calls**

Threat calls will provide Members an overview of the key cyber threat landscape developments including the latest tactics, techniques and procedures used by adversaries

Members will learn more about the:

- Key cyber threats and incidents impacting Critical Information Infrastructure and industrial organizations; and
- Key critical vulnerabilities released and the how adversaries are exploiting them.

# OT-ISAC Capabilities

## SUCCESS STORIES

OT-ISAC aims to help CII sectors boost their Cyber Defence Readiness by accelerating information sharing and adoption of essential OT cybersecurity best practices and benchmarks, including providing relevant and actionable threat information and building trust among stakeholders.

### OT Threat Modelling

OT-ISAC supported a member developing a threat model for their critical OT assets based on industry best practices and frameworks. High level activities included conducting a network architecture review, enumerating threat events based on STRIDE and modelling the attack based on ICS Cyber Kill Chain and MITRE ATT&CK. The initiative helped the member identify potential threats and vulnerabilities and inform risk mitigation efforts.

### OT-ISAC Support

OT-ISAC supported multiple members' requests for information over the past year.

These included the enrichment of malware signatures, assessment of vulnerabilities and insights into the latest threats impacting industrial organizations and critical services.

### OT-ISAC Training

OT-ISAC conducted a half day security awareness training for over 35 member participants on the fundamentals of OT cyber security.

The training covered the latest threats to OT assets, industry standards and best practices and specific recommendations to reduce cyber risks based on real world challenges faced collectively by the OT-ISAC community.

# What to expect

**As we move forward in this journey, OT-ISAC growth strategy includes innovation programmes, forging partnerships and strengthening relationships with Asset Owners, Operators, Government, and other stakeholders in developing CII ecosystems around the region.**

**Establish OT Incident Response Committee**

**Create Sector Workgroups and Facilitate Sector Specific Forums**

**OT-ISAC Academy**
*(OT Awareness Training and Workshops)*

Upcoming 16 events in 2021 and flagship

## OT-ISAC APAC Summit

*September 2021*

## Expand beyond Singapore into Asia-Pacific

Onboarding more members in 2021

Continue to build cross-border partnerships

# Milestones and Achievements

## Partnerships

AUSCERT

## Community Engagements

*"OT-ISAC Virtual Summit gathers key expert for OT/ICS Security"*


**656** Attendees

**Profiles:**

- End Users: 42%
- Government: 20%
- Vendor: 21%
- Others 17%

**21** Total Events

- 11 Webinars
- 3 Conference Presentations
- 7 Threat Calls

*Monthly Threat Calls & Members Meetings*


*"I thought the threat calls have been very informative and given good insight on the various vulnerabilities which even users may not be aware of at the moment"*

*"It's quite informative to know about current/ recent threats or attacks that are happening around the world, as well as the latest vulnerabilities and the recommendations that we can adopt.*

*It is good that there is a summary of the key major cyber incidents that happened around the world."*

*I found that sessions are useful and relevant to OT products, environment and threats.*

*"Good session. Overviews and high level alerts are good."*

# OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

## Why Join OT-ISAC?

*"Cybersecurity success or failure hinges on the ability of people, organizations and industry sectors to share information."*

- Receive alerts on the latest threats impacting Operational Technology and Critical Information Infrastructure
- Gain access to intelligence (indicators of compromise, Dark Web monitoring, finished reports) shared by trusted members and partners within the OT-ISAC community
- Leverage the capabilities of our OT-ISAC analysts and trusted partners to analyze threats and mitigate potential attacks, including cross-sector sharing with other affiliated ISACs/ISAOs
- Enhance the threat intelligence capabilities of your organization
- Participate in exclusive research initiatives to uncover the threats and vulnerabilities in your OT environment
- Gain access to OT cybersecurity trainings and exercises to enhance the cyber capabilities and awareness of employees in your organization

### BE PART OF THE OT-ISAC COMMUNITY!

For details and inquiry about membership in OT-ISAC, email us at info@otisac.org

LEARN MORE AND VISIT WWW.OTISAC.ORG OR SCAN BELOW:

Powered by: GLOBAL RESILIENCE FEDERATION