

Eastern Canada ICS/OT Cyber Community

Inaugural Committee Meeting – January 2026



Agenda

- 0. Context**
- 1. Introductions – all**
- 2. Background – Peter**
- 3. Open discussion**
- 4. Key formalization decisions**
- 5. AOB**



0. Context

- **Eastern Canada ICS/OT Cyber Community**
 - *Members will engage with professionalism, respect, and openness to diverse perspectives.*
 - *All discussions will follow the Chatham House Rule and/or TLP to protect confidentiality and build trust.*
 - *Participation will remain educational, collaborative, in good faith, and not sales-driven*
 - *Contributing members will focus on practical, actionable insights that strengthen Eastern Canada's ICS/OT community.*



Our Charter:

Building Stronger Cyber Resilience

Join us in fostering trust, collaboration, and knowledge-sharing among ICS and OT practitioners across Canada for a more secure future.

Objectives

- Share lessons learned, emerging threats, and best practices to enable Canadian practitioners and industrial organizations
- Build cross-sector connections in utilities, manufacturing, transportation, and critical infrastructure
- Provide a vendor-neutral, non-commercial space for open discussion
- Explore opportunities for collaborative initiatives (exercises, info-sharing, collective defense)
- Educate and enable Canadian practitioners in understanding ICS/OT-specific challenges and growing the Canadian body of ICS/OT cybersecurity knowledge.

Scope

- Focus: Industrial organizations/practitioners operating ICS and OT systems
- Region: Aligned to Eastern Canada with links to national/international efforts
- Exclusions: Activities primarily driven by sales or marketing interests

Membership

- Open to asset owners, operators, academics, government employees, and supporting organizations including service and tech providers
- Participating is voluntary; members follow the Chatham House Rule (information may be shared but not distributed) and or TLP (typically TLP: Green or TLP: Amber)

Meetings

- Quarterly, monthly, or bi-monthly session (mainly virtual to start).
- Mix of presentations, discussions, and knowledge-sharing.
- Future: hosted hybrid (physical & remote) on a rotating basis where feasible.

Neutrality Trust Collaboration Practicality

Code of Conduct:

Members will engage with professionalism, respect, and openness to diverse perspectives. All discussions will follow the Chatham House Rule and/or TLP to protect confidentiality and build trust. Participation will remain educational, collaborative, in good faith, and not sales-driven while contributing members will focus on practical, actionable insights that strengthen Eastern Canada's ICS/OT community.

1. Introductions



2. Background



Basis for Canadian community

- NZ ICS Cyber Technical Network
- Representatives from owners, operator and service provider organisations with an interest in ICS Cyber Security in NZ.
- An industry-led organisation established to promote the sharing and understanding of Industrial Control Systems (ICS) Cyber Security ideas in order to foster learning, development and improve cyber security maturity for NZ industrial companies.
- <https://icscyber.org.nz>



TLP: WHITE (UNRESTRICTED)



TLP: WHITE (UNRESTRICTED)
Information may be distributed publicly without restriction.

NEXT EVENT:
Thursday 28th May 2020, 12:00-1400

Michael Lagana, ICS Cybersecurity Consultant, Claroty on 'Secure Remote Access for OT (under the hood)'
Glen Willoughby, Digital Innovation Advisor, NASA JPL on 'Utilising Emerging Technologies to Secure Critical Infrastructure'
Jim Scott, ICS Security Consultant on 'Cloud computing business methodology for OT'

Register at <https://icscyber.org.nz> for remote access instructions. Note: No physical location for May 2020 forum

PURPOSE/AIM:
An industry-led organisation established to promote the sharing and understanding of Industrial Control Systems (ICS) Cyber Security ideas in order to foster learning, development and improve cyber security maturity for NZ industrial companies.

AUDIENCE:
Representatives from owners, operator and service provider organisations with an interest in ICS Cyber Security in NZ.

GROUND RULES:

- NCSC Traffic Light Protocol to be used for all information transfer (primarily TLP: GREEN)
- Specific company standards and practices will not be shared unless approved in writing by the company.
- No commercially or contractually sensitive information will be exchanged or discussed (although vendors may be invited to attend and describe their solutions and approaches to ICS Cyber Security).
- The information shared is intended to educate and promote learning. The steering committee will accept no liability resulting as a use of the information or offer any guarantee of the accuracy of the information.

2019 Forum Talks included:

- Fast-Tracking Defence-in-Depth
- A Tale of Two Hats
- Control Systems in the Cloud
- The Value of ICS Visibility Within a SOC
- NCSC – Thinking Ahead. Being Prepared
- The TTPs of Hard Hat Incident Response
- VCSS-CSO Analysis and My Journey
- Cyber Security Strategy for ICS Systems
- Risk Based Approach to Security

2019 NZ ICS Cyber Summit Talks:

IDENTIFY: Getting the Foundations Right!
PROTECT: Building on strengths
DETECT: Malware Free Networks – scaling cyber threat detection and disruption, NCSC
RESPOND: Do Your Homework Before It's Due!
RECOVER: The Need for Intel-Driven Defense for Proper Root Cause Analysis and Recovery

Register at <https://icscyber.org.nz> or email info@icscyber.org.nz for more information



TLP: WHITE (UNRESTRICTED)
Information may be distributed publicly without restriction.



IN ASSOCIATION WITH:
SANS ICS ECL Cyber



NZ ICS Cyber TN – Ground Rules

1. NCSC Traffic Light Protocol to be used for all information transfer
 - Assume TLP: GREEN – Share within sector; Not public
2. Specific company standards and practices will not be shared unless approved in writing by the company.
3. No commercially or contractually sensitive information will be exchanged or discussed (although vendors may be invited to attend and describe their solutions and approaches to ICS Cyber Security).
4. The information shared is intended to educate and promote learning. The steering committee will accept no liability resulting as a use of the information or offer any guarantee of the accuracy of the information.

NZ ICS Cyber TN – EXAMPLE Call to Action

- 2025 Online/Hybrid/In-Person Forums
 - ~August: in-person lunchtime forums (Fortinet)
 - ACTION: Let us know speakers/topics you want to hear
- 2025 NZ ICS/OT Cyber Summit
 - WED 26th Nov in New Plymouth – full-day in-person only
 - ACTION: Save the Date + send your ideas
 - Community effort – by the people, for the people
 - ACTION: Need committee members, presenters, exhibitors, panellists, round table facilitators, scholarship nominations.... and ideas!
- <https://icscyber.org.nz> or info@icscyber.org.nz



3. Open Discussion



4. Key Formalization Decisions

- Name**
- Format**
- Cadence**
- Intent**
- Committee**
- [Anything else?]**



5. AOB

