Canadian Cyber Threat Exchange
Informing Canadian Business

Échange canadien de menaces cybernétiques
Informer les entreprises canadiennes

Terms of Reference – Threat Intelligence Committee

1. **Introduction**
   - The Terms of Reference (ToR) will serve as the committee's guiding document, outlining its purpose, membership, roles and responsibilities, meeting cadence, and processes for decision-making and reporting.

2. **Purpose and Scope**
   - The purpose of the Threat Intelligence Committee (TIC) is to:
     i. Openly share threat intel and mitigation strategies amongst the TIC so that participating TIC organizations will be more secure because of it.
     ii. Provide context to threat intelligence.
     iii. Disseminate information.
     iv. Analyze and comment on incidents and impact assessments.
     v. Provide threat and high-level mitigation information to CCTX membership through presentations, portal alerts, and webinars as appropriate.
     vi. Provide the bi-weekly recommendation on the Canadian Cyber Threat level.

   - The scope includes:
     i. All threats to systems, networks, and information.
     ii. Includes all industry sectors.

3. **Membership**
   - As the CCTX is cross-sectoral, the goal of the TIC membership should be the same.
   - Membership shall be capped at two per company, where one is primary, and the other is the backup.
   - The Threat Intelligence Committee will comprise participants from the Member organizations only; and the CCTX (Executive Director, Strategic Advisor, COO, and Technical Lead).
     i. TIC member organizations must be an Associate[1] or Member-level participant in the CCTX.
     ii. All participating organizations must have an active CCTX membership.
   - When participating in the Threat Intelligence Committee, it is important to consider various criteria to ensure effective collaboration and decision-making.
     i. Expertise: Committee members should possess expertise in threat intelligence, cybersecurity, risk assessment, or related fields. This ensures that discussions are informed and productive.
     ii. Industry Knowledge: Members should have a deep understanding of the industry in which the company operates. This allows for the identification of industry-specific threats and vulnerabilities.
     iii. Analytical Skills: Strong analytical skills are crucial for evaluating threat intelligence data, identifying patterns, and drawing meaningful conclusions. Committee members should be able to analyze complex information effectively.

[1] https://cctx.ca/membership/

iv. Communication Skills: Effective communication is essential for sharing threat intelligence findings, discussing potential risks, and collaborating on mitigation strategies. Committee members should be able to articulate their ideas clearly and listen actively.
v. Collaboration: Committee members should be willing to work collaboratively with others, sharing information and insights openly. This fosters a culture of teamwork and ensures that the committee functions smoothly.
vi. Proactive Mindset: A proactive mindset is crucial for threat intelligence. Committee members should proactively identify emerging threats, stay updated on the latest trends, and propose proactive measures to mitigate risks.
vii. Decision-making Skills: Committee members should possess strong decision-making skills to evaluate different options, assess risks, and make informed decisions. This includes considering the potential impact of decisions on an organization's security posture.

4. Adding or Replacing members

- When a primary member is no longer available such as due to a role change or illness, if available the backup will assume the primary role and another company member will be proposed as a backup.
- Voting will occur when new or replacement members are proposed. The CCTX and both the primary and backup for member organizations are eligible to vote.

5. Roles and Responsibilities

- When these Terms of Reference were written, roles such as Chair, Vice Chair, and Secretary were not named, nor proposed. If the TIC membership proposes such roles, there will be a vote such as in #4.
- All TIC members are treated and respected equally.

6. Meetings

- The meeting will be bi-weekly on Fridays at 11 AM EST, unless the Friday is a stat holiday, or an ad hoc meeting is scheduled given threat trends.
- The meetings will be online.
- The standing agenda is roundtable sharing in support of the TIC Purpose and Scope. However, a member can propose an agenda item prior to, or at the beginning of, a meeting.

7. Decision-Making

- Decision-making is enabled through a question proposal and an ensuing vote.
- When voting can be completed prior to a meeting, such as voting on the Canadian Threat Level, an email will be sent to all TIC members asking them to vote. Each member can provide a vote with an email response.
- If voting is required during a meeting, all attending members are entitled to a vote and can do so with a written response (email, message), gesture such as the raising of the hand, or verbally.
- A vote of 51% of the attending members is deemed accepted.
- If there is a conflict, the CCTX will recommend a resolution.

8. Communication and Reporting

- Collectively, the TIC provides wisdom to membership. The CCTX will share this wisdom via the appropriate channel(s) such as the CCTX Portal or email, or by asking a TIC representative to present the wisdom, such as during a weekly call or a Webinar.
- The TIC members are encouraged to collaborate during the TIC meetings and throughout the week via the group email address - CCTXThreatIntelligenceCommittee-TIC@cctx.ca.

9. Confidentiality and Security

- TLP Version 2[2] will apply to the business of the TIC.
- TLP Red conversations within the TIC shall not be shared outside of the TIC, unless agreed upon by the TIC.
- The default for TIC meetings is TLP Amber.

10. Evaluation

- The TIC is deemed effective if more-often-than-not:

  i. the TIC collaboration is evident;
  ii. the TIC recommends a Canadian Cyber Threat Level bi-weekly; and,
  iii. the TIC provides guidance to the CCTX membership.

Document Title: Terms of Reference – Threat Intelligence Committee

Version: 2.0

Last Updated: March 8, 2024

Updated By: Rick Ouellette

Change Description: Second draft

---

[2] Traffic Light Protocol (TLP) (first.org)