TF-CSIRT Cyber Threat Intelligence Working Group

CTI WG

Roderick Mooi, GÉANT

Head of TF-CSIRT CTI WG (Coordinator)

70th TF-CSIRT Meeting, Stockholm

26 September 2023

What and why → How?

[Jan Kopriva proposed at 68th TF-CSIRT meeting (Bilbao); SC Approved]

"It would be up to this WG to ***figure out what and how we might share*** within TF-CSIRT, since although there are some CTI exchanges already in place we currently lack any TF-CSIRT-wide approach to this area."

Objective:

- develop a framework(s) for improved TF-CSIRT community approach to CTI
- increased information exchange

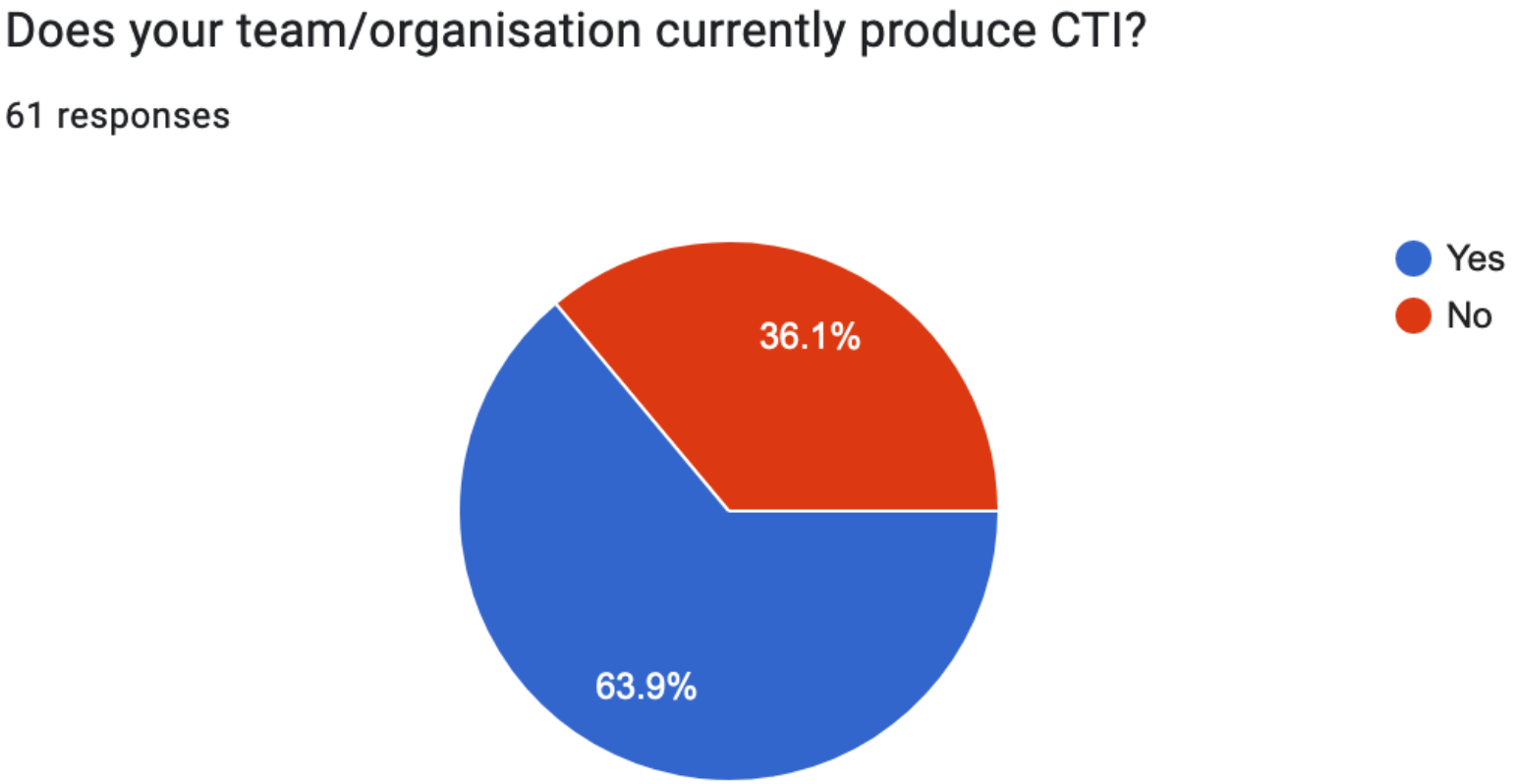
Proposed Goals

- Identify an optimal **technical solution** for exchange of CTI between TF-CSIRT member teams
- Develop **processes and policies/guidelines** governing the exchange of CTI within TF-CSIRT
- Possibly: participate in FIRST CTI SIG on behalf of TF-CSIRT in some way
- ?

Our journey so far

- Launched at 69th TF-CSIRT meeting + 1st meeting
- Two virtual meetings in-between
- Lots of discussions on tools, trust, sharing, producing and consuming CTI
  - MISP
  - Sensitive data > Trust + TLP
  - Some can share easier than others (regulated)
  - Plenty feeds but quality is a challenge
  - Create and share within TF-CSIRT
- -> CTI Survey : 61 respondents ☺

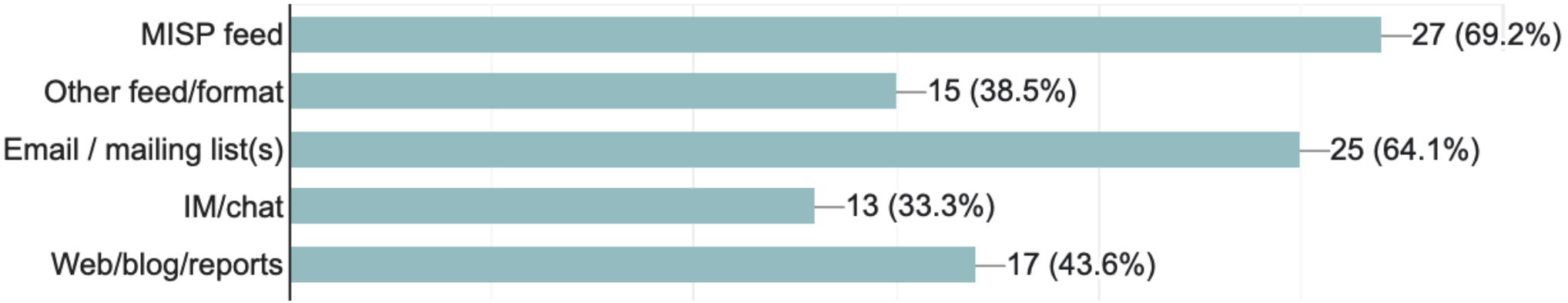
CTI Survey



For those that answered “No”: 75% plan to > 90%!

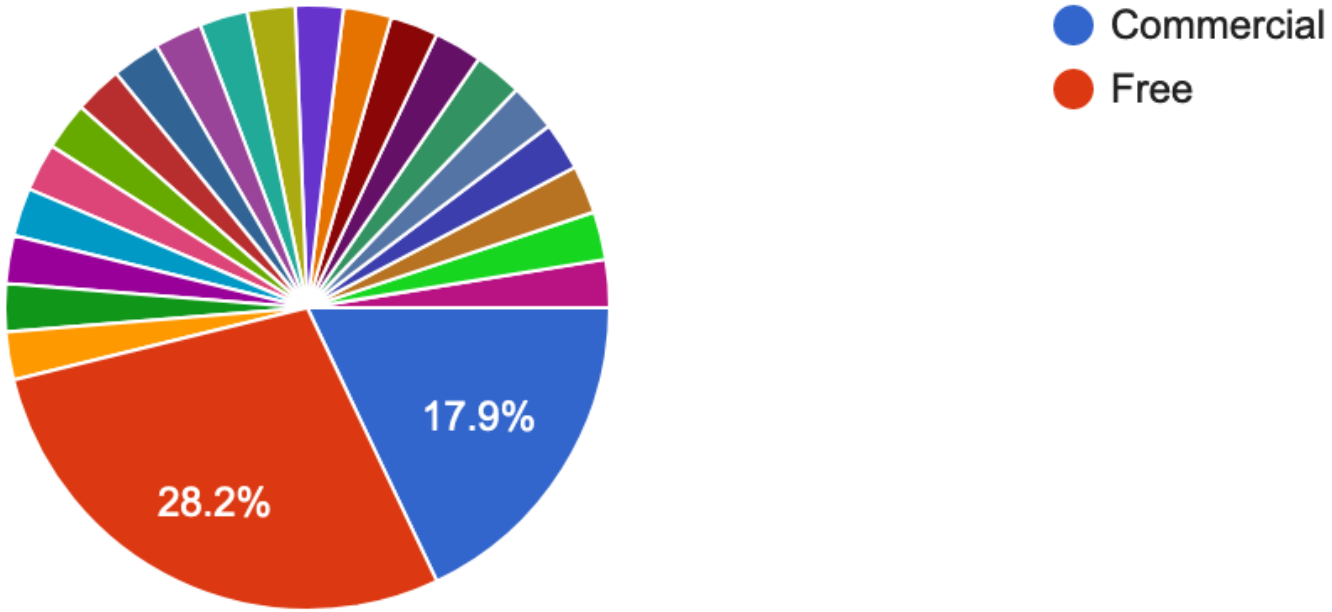
By which mechanisms do/could you share (select all that apply)

39 responses



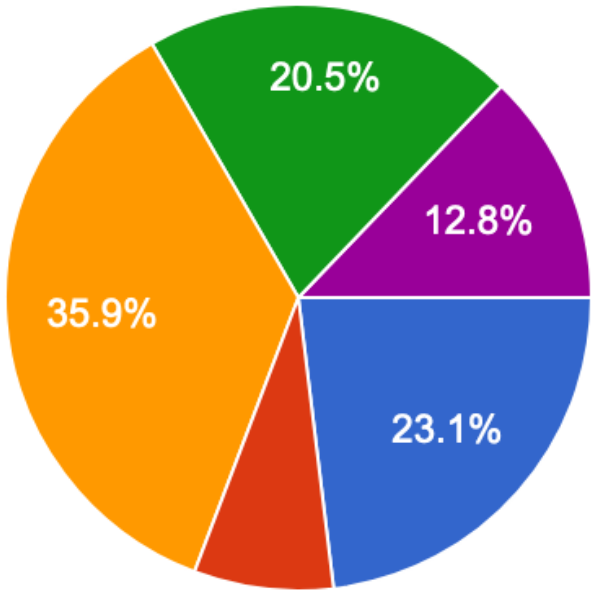
Is your CTI available commercially (paid for) and/or free?

39 responses



Can it be shared with the TF-CSIRT members?

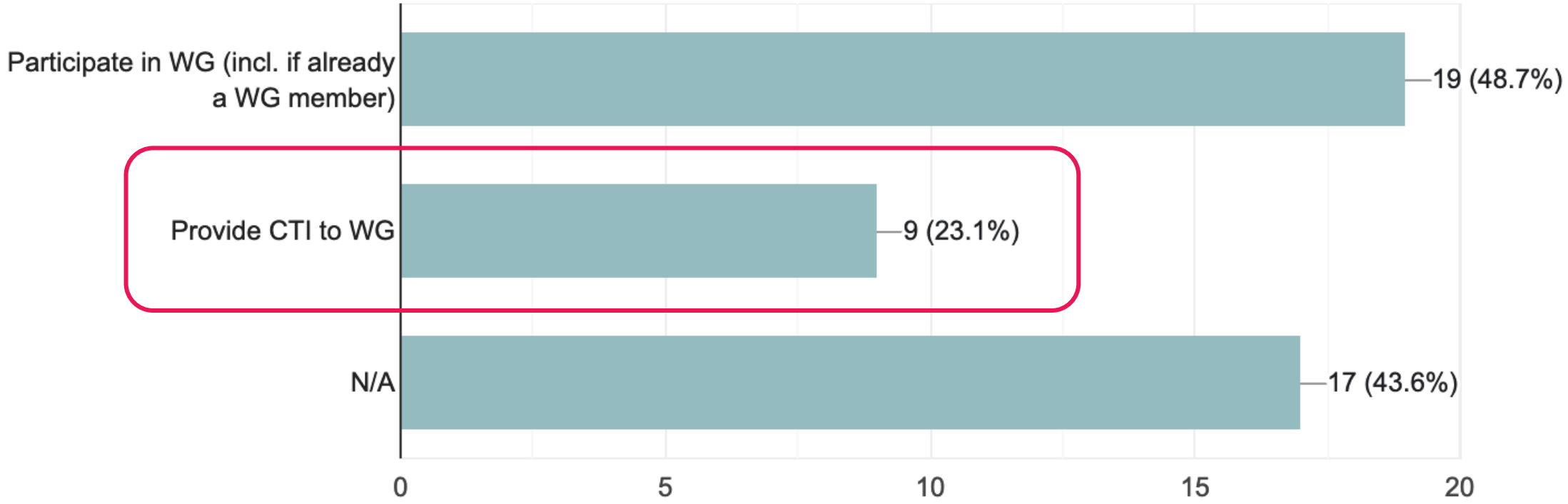
39 responses



- Yes, all teams
- Yes, only accredited and certified teams (assumed TLP: AMBER)
- Yes, but with restrictions. Explain: ...
- Yes, but limited constituency (e.g. within country; only for specific sector). Define: ...
- No, regulated or similar limitations
- No, we can't share. Please expand: ...

Would you like to participate in and/or make your CTI available to the TF-CSIRT CTI working group as a pilot for broader TF-CSIRT dissemination/adoption?

39 responses



Interested?

- Meeting today at 16:00 (after the main session)
- Request to be added to CTI WG mailing list:
  → ti@trusted-introducer.org

Thank You

roderick.mooi@geant.org

www.geant.org

Co-funded by
the European Union

GÉANT