|  |  |
| --- | --- |
| **STRENGTHS** | **WEAKNESSES** |
| * TRUST
* Openness of the community
* TF-CSIRT meetings: networking, P2P communication, ability to get to know other people
* Brings together CERTS from all areas (gov/nat/edu/com) to exchange in an all-inclusive way
* Size of the community
* Exchange of ideas, experience, best practices, tools; getting new perspectives, keeping up with trends
* TI database (with an API), TI certification, communication tools (mailing list, crypto remailer, etc)
* TRANSITS
* Reaction test
* Cost effective
 | * Content of TF-CSIRT meetings – presentations of very different quality, plenary sessions do not encourage interaction
* No full time staff – cannot ask too much from a community ran on a voluntary basis
* Listing as lowest membership category is abused as rubberstamp and seen sufficient by many teams who do not aim to get accredited
* Suffering “success-disaster” – used to be very successful, now difficult to keep up
 |
| **OPPORTUNITIES** | **THREATS** |
| * Involve community to get better content for the meetings (Programme Committee, more input of local host), introduce lightning talks, organise more group sessions, short, practical trainings, parallel sessions for specific development topics (e.g. IntelMQ-related), and sharing content in smaller groups (e.g. lessons learned from recent incidents)
* Create subgroups (working groups), e.g. one for software/tool development
* Assign mentoring teams for new teams for their first meeting, continuing introductions for new team members (TI 101)
* Closer collaboration with ENISA, NIS, FIRST, EU directive; more involvement in sector based CSIRT coordination
* Issue public statements on different topics, comment on initiatives on the website
* Promote MISP platform together with CIRCL
* White box solution (baseline) e.g. for national teams/groups
* Add more TRANSITS topics and streamline with ENISA and FIRST content
* Involvement in actual operational support – some teams could help others in implementing operational capabilities, TI could be coordinating such activities
* More visibility for TI – invest in PR activities, provide material to encourage mature teams to promote its services and community in their region/country
* Create material on the value of TI that teams can use for their management and constituencies
* Extend contact database to include global service providers that are hard to approach and team capabilities that can be used/rented by other teams – “outsourcing” can be better than building in-house capability
* Investigate possibilities of separating from GEANT (eventually, not immediately)
 | * New participants do not find the content attractive
* TF-CSIRT crowd not very sociable with new teams
* Teams do not have the budget to get accredited
* Growth of the community might impact the level of trust
* Geographical scope is getting too large and contains untrustworthy countries
* The EU directive network between CERTS can reinvent solutions that the community already has
 |

**TENDER:**

* Currently the community part is left outside the tender – consult the lawyers on how to reflect the “community factor” that in the tender
* Specify trust level as a formal requirement
* Insure low flexibility of changes - the service portfolio particularly has to be defined for years ahead
* The tender should be specified in such a way that would prevent unwanted bad outcomes where an incapable service has to be chosen for legal reasons of the tendering process
* Add secure wiki (like Etherpad) or file server to service portfolio
* Instead of tendering, investigate whether GEANT can hire TI staff directly

**SERVICES:**

* CHIHT was useful – could it be brought back?
* The mailing list (crypto remailer) is not used for sharing data as often as it could be
* Services that are not used: OOB notifications, Secure chat, IRC (very few use it, some did not know about it at all)
* Useful services: teams’ directory, accreditation/certification, irt object management, general mailing list, teams rep web interface, SIM3

**LISTED TEAMS:**

* To encourage accreditation of more listed teams, introduce various participation fees (based on country, type of organisation, SC approved exceptions)
* If money is the problem, make exceptions for accreditation fee based on the income of the team
* Introduce email checks for listed teams - mark some of those “inactive”
* Rename “listed” teams to “non-accredited”
* Only have accredited teams and non-members (get rid of “listed” category altogether)
* Make the list of listed teams only visible to accredited teams so that the public could not verify listed status and thus not infer any status or quality statement from that
* Ask listed teams to pay a contribution for attending the meetings