Listed Teams Discussion Session at 50th TF-CSIRT Meeting

Background

At the 49th TF-CSIRT meeting a presentation outlining a recent survey of listed teams and their engagement in the community. As a result of this, it was decided that break-out groups at the 50th TF-CSIRT would discuss the current issues with listed teams and how the service and engagement could be improved. A series of questions were posed to 7 break-out groups.

Recommendations

The following recommendations are made based on the summary of the group discussions:

1. Listed teams should remain a service within the TF-CSIRT portfolio with no change to the name and with the same services offered to the teams as currently provided .
2. A better definition of what is meant to be "listed" should be developed (possibly with more promotional-style material) and abuse of this definition should be monitored.
3. Listed teams should be fully relisted after three years, including renewing the sponsorship stages.
4. The TI database should remain fully public.
5. Listed teams should participate in response testing at least once per year.
6. Non-responsive teams should be flagged / greyed out on the TI database.
7. Listed teams should be actively encouraged (required?) to attend the first TF-CSIRT meeting after their listing, and present their team.
8. An enhanced role should be established for the sponsors – they should be listed on the team profile prominently, they should help encourage the team to attend meetings and participate in the community and they should be involved in trouble shooting problems with non-responsive teams.

Summary of Questions

The following questions were asked to groups at the 50th TF-CSIRT meeting:

1. Should there be a time limit on the duration for listing?

2. Should PGP keys be mandatory for listed teams?
3. Should the name "listed" be changed?
4. Should there be more restrictive requirements for listing?
5. Should we keep listed teams?
6. Should the directory be non-public?
7. Should there be a fee for listing?
8. Should there be more services for listed teams?
9. Should accredited teams pay more to support listed teams?
10. Should there be mandatory response testing?
11. Should we exclude non-responsive teams and how do we better engage teams?
12. What is the role of the listed team sponsor?

Summary Overview:

	Question	Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Summary
1	**Limit Duration for Listing**	Yes – with a way to regain support	More important to have some sort of contact	Yes – max 3-4 years. Should be active in some way in first two years (attend meeting, presentation, contribute to mailing list)	The goal of TI is to have a directory (as complete as possible) about CSIRT teams in Europe/around. Therefore it should not be made any more difficult for new teams	To get the best coverage and ensure the availability of PoC information there should be no limitation based on fees or limited duration of the listed	Yes, 2 – 3 years	Yes – restart the listing process after three years.	*Most groups supported some sort of limitation on the listing period – the most favoured suggestion was to re-start the listing process after 3 years.*

					to get listed and there should be no fee for listed teams. Also no limited duration.	status. To ensure quality, - renewal of listed status every three years (same process as for new listing candidates)			
2	**mandatory PGP keys for Listed Teams**	Nice but not feasible	Irrelevant – trust is built by dealing with team	Mail signature and encryption should be in place – either PGP or X.509.	No		Yes		*There was no significant support for mandatory PGP.*
3	**Change listing name**	No, rather emphasize what it means to be listed	Better alternative would be to make Listing mean something better. Maybe just drop the name? Or make it clear on the web site what it	"Candidate since YYYY", where YYYY is the year of listing. "Applying"	Changing name for listed teams – some people said it does not matter, but there was a suggestion to rename it to "CSIRT wanabees".	The term used to name the "listed" teams shall be positive (therefore "not accredited" is exactly the point, but not nice). However something less like "known"	Junior or novice, accreditation candidate TLP status two flavors of listing, white and green	No, name is OK. Need to make it clearer what listed means. Hinder misuse and misinterpretation of listed status e.g. for PR use or public tenders	*There was no consensus on the naming issue, although a better definition of what listing means was recommended by several groups.*

			means? Show sponsors on public web site.			would be okay.			
4	**More restrictive requirements for listing?**	No	No (but make constituency mandatory)	Teams should provide an official commitment/letter of intent to be accredited by YYYY-MM, where YYYY-MM is the date of team's choice. More sponsors does not mean more trust. Transfer part of responsibility to sponsor.	It is important that data are accurate. 1/year checking of contact information is very important. Update of the info should be possible without certificates – just clicking on a long URS for example. Also for each listed team it would be nice to add info when the info is updated for the last time.		yes it so easy to become "listed" -if you sponsor and teams misbehave, you have to be impacted -define what misbehave means		*There was no consensus on this question, but other recommendations to support "better" listing are made elsewhere*

5	**Keep Listed Teams?**	Yes	Yes	Yes, but as a step to accreditation.	Yes	Yes	Yes	Yes	*There is consensus support to keep listed teams in TI.*
6	**Non-public Directory?**	No	No	No, if the teams will be called more properly, such as a candidate.	The directory has to remain open and public, it is used also by security researchers and CSIRTs from all over the world.	The value of the directory is also defined by its availability to other CSIRTs around the world. There might be some abuse of the term "listed" but still it is important to make the information available.	No	Maybe complete directory should only be made available for accredited teams	*The majority of teams felt the directory should be public.*
7	**Fee for Listing?**	Symbolic fee	Some Listed teams already pay for GÉANT fee. (NH: only 3!)	No, or a small one-off fee	there should be no fee for listed teams.	As long as there are no other services provided (to update the team information themselves is actually a	maybe to green status / one of listed layered status	Do not have to pay but show that they are alive Maybe a small symbolic annual fee, first 2-3 years for free	*There was no consensus on fees for listed teams.*

						service they offer to us for free ;) no fee should be taken. An initial fee is way more expensive from an administrative perspective than it would do any good _____ There was the notion that listed teams need help (budget) to participate in TF-CSIRT meetings.		Fee will invoke more internal discussions in the listed team itself	
8	**Services for listed teams**	As now, for free	As now, for free	Current services are OK. Mentoring of the listed teams should be done by their sponsors.	It is not necessary to involve listed teams in the community and no additional services				*The majority of groups felt that the services offered to listed teams should remain the same*.

					should be provided, just the bare minimum – as now. No reaction tests, no PGP keys, etc.				
9	**accredited teams pay more to support listed teams?**	No	No	N/A.	Fee – people want to know how much each team is paying for the listing process to be able to give feedback on this topic.		we need more information what are listing costs one time cost for listing and yearly membership fee		*There was no consensus on this issue.*
10	**Mandatory response testing?**	Yes but just once a year	Yes	Yes	It is not necessary to involve listed teams in the community and no additional services should be	Yes – but with no specific sanctions, follow-up	Yes	Yes	*There was consensus that listed teams should participate in mandatory response testing*.

					provided, just the bare minimum – as now. No reaction tests, no PGP keys, etc.				
11	**Exclude non-responsive teams / better engage teams**	Yes, or "grey out" on website	Yes, but keep historical data or put a mark on the listing	Yes but after another check. Actively invite them to meetings – they should present their services, cases etc..	It is important that data are accurate. 1/year checking of contact information is very important. Update of the info should be possible without certificates – just clicking on a long URS for example. Also for each listed team it would be nice to add info when the info is updated		Yes, exclude after third time share information and make dedicated presentation to participate once in TF-CSIRT meetings in two years	Yes	*Most teams supported some sort of flag on the TI database to show that teams were non-responsive.* *Listed teams should be invited to present at meetings – perhaps at the first meeting after listing?* *Listed teams should show some sort of engagement via the mailing list, meetings, presentations etc.*

					for the last time.				
12	**Role of sponsors**	But more emphasis on this, list name of sponsors, use them to trouble shoot problems	But more emphasis on this, list name of sponsors, use them to trouble shoot problems	Listed teams are responsibility of the sponsors. Their sponsor should take care of them and invite them to the meetings and explain what TI/TF-CSIRT community is.	Not in notes.	number of sponsors can be increased as we now have a much higher number of potential sponsors.	-if you sponsor and teams misbehave, you have to be impacted -define what misbehave means		*Most groups supported a broader role for the sponsors: list them on the profile for listed team, ask them to help with inviting teams to meetings, use them to help trouble shoot.*