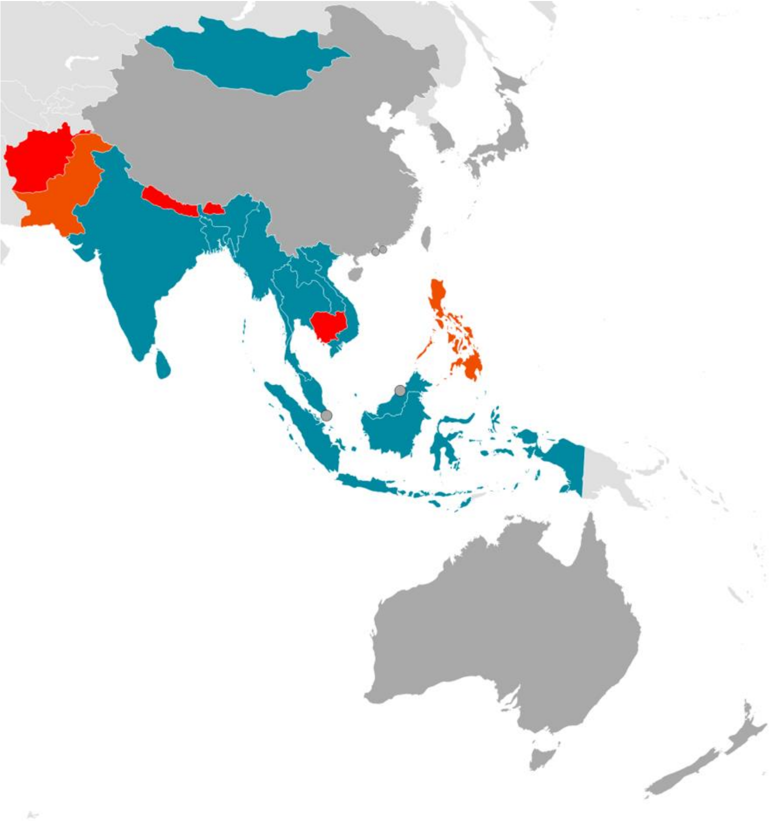
CSIRT Capacity Building in Asia

1 General Information

Title of proposal – CSIRT Capacity Building in Asia: Providing Security Trainings and Facilitating Creation of a Trusted Information Sharing Platform
Relevance of Work Package(WP) – WP3
Duration – 2 years (January 2018 – December 2019)
Relationship with other existing projects – Follow up of the CSIRTS in Asia project (Grant Contract ACA 2016/376-562). The TRANSITS course materials have been collaboratively developed by members of the GÉANT's task force TF-CSIRT with support from ENISA.
Keywords – training, network security, CSIRT, CERT, train the trainer

Regional diversity – NRENs (or equivalent organizations) from 16 beneficiary economies (Bangladesh, Bhutan, Cambodia, India, Indonesia, Laos, Malaysia, Nepal, Pakistan, Philippines, Sri Lanka, Thailand, Vietnam, Afghanistan, Mongolia and Myanmar) will be invited to send funded participants to the trainings and meetings, focussing primarily on those that do not have a fully functioning CSIRT team (RED: Least Developed Countries (LDCs) and ORANGE: Lower Middle Income Countries and Territories).



The remaining Asi@Connect participant economies (Australia, China, Hong Kong, Japan, Korea, Singapore, New Zealand) will be offered unfunded places at the training and invited to attend the Information Sharing meetings.

2 Information on the participants

2.1. Principal Investigator(PI)/Leader

Sigita Jurkynaitė, GÉANT Project Development Officer, Singel 468D, 1017 AW, Amsterdam, The Netherlands, +31613997185, sigita.jurkynaite@geant.org

Sigita is one of the Project Development Officers at GÉANT who manages and supports security related projects and working groups, including TF-CSIRT (task force promoting collaboration and coordination between CSIRTs in Europe), SIG-ISM (a forum for interchanging knowledge and experiences on information security management topics), WISE (global e-infrastructure security experts' forum), Global NREN Security Group (an international forum for senior NREN security professionals, sponsored by the Global NREN CEO Forum) and Academic Security SIG of FIRST. Sigita was one of the GÉANT staff members who carried out the CSIRTs in Asia meeting and Mini-TRANISTS workshop at APAN44 in Dalian, China, funded by Asi@Connect. Sigita has experience in supporting TRANSITS and other security courses and has contacts in a world-wide network of experienced trainers.

2.2. List of Collaborating Participants[1]

No.	Name	Organization	Economy	Email
1	Jamie Gillespie	APNIC	Australia	
2	Don Stikvoort	Head Trainer TRANSITS	Netherlands	
3	Melanie Rieback	Radically Open Security	Netherlands	
4	JP Velders	University of Amsterdam	Netherlands	

3 Proposed Activities/Programs

3.1. Overview/Background

The wider deployment of eduroam® and eduGAIN™ services throughout the Research and Education community assumed that the NREN (or similar organization) supporting those services was also responsible for the operation of a Computer Security Incident Response Team (CSIRT). While it is the case Europe, where TF-CSIRT (task force promoting collaboration and coordination between CSIRTs in Europe) supports 72 CSIRTs from the R&E community, the situation in Asia Pacific region is very different. No CSIRT operates in six Asi@Connect partners (Afghanistan, Pakistan, Nepal, Bhutan, Cambodia and Philippines) and the support for the R&E community in the rest of their territory is not always clear.

[1] The list might change depending on the availability of the trainers. Around 50 experienced TRANSITS trainers from 15 economies can be approached depending on the expertise required.

For that reason, in June 2017 GÉANT submitted a project proposal to Asi@Connect, titled 'CSIRT Asi@Connect and Mini-TRANSITS' (under WP2: Capacity Development of Developing Country NRENs), aiming to create a gap analysis within the Asi@Connect region in order to better support incident response and ensure that the R&E institutions have the skills and knowledge needed to run a fully functional CSIRT.

As part of APAN44 in Dalian, China in August 2017, a CSIRTs in Asia meeting and Mini-TRANSITS workshop was offered, initially targeting six Asi@Connect beneficiary economies currently without a CSIRT. However, the meeting and the training have proven to be exceedingly popular - across both events there were a total of 46 people from 14 economies representing 34 organizations.

During the CSIRTs in Asia meeting, the attendees identified continuing development requirements in the areas of: Building Trust, Capacity Building & Information Sharing; to support their security incident readiness and support for deployment of federated services such as eduroam® and eduGAIN™ throughout their communities. The Mini-TRANSITS one-day training provided was overwhelmingly rated as "Very Useful" in the survey conducted after the meeting. 90% of the attendees indicated that they would certainly like to attend similar events in the future. Participants expressed the need for a longer in-depth training that would cover a wider range of topics and noted that APAN conferences would be good events to collocate regional CSIRT meetings and trainings with.

The interest from this initial meeting and workshop makes it clear that there is a need for CSIRT co-ordination, development, training and information sharing within the Asia-Pacific region and funding should be allocated to support further engagements at APAN45 and beyond. Therefore, we are proposing a series of 'CSIRTs in Asia' events, combining meetings and TRANSITS I trainings, to be held throughout two years. The meetings would serve as a platform for sharing information, experiences and knowledge in a form of presentations, discussions and demos. The trainings would consist of four modules: Operational, Organisational, Legal and Technical, which form knowledge basis for CSIRT personnel. 'CSIRTs in Asia' meetings would be a unique opportunity for the participants from the beneficiary economies to network with their peers, discuss security issues in a trusted environment and be tutored by well-known security experts. The events will also have the train-the-trainer function – after attending, the participants will have the knowledge and the materials needed to bring the TRANSITS subjects to their home institutions.

3.2. Objectives

- Creating a self-sufficient trusted network in Asia-Pacific region for R&E security experts;
- Providing affordable, state of the art high quality training to CSIRT personnel in the region;
- Equipping the attendees with the knowledge and materials needed to give security trainings in their constituencies.

3.3. Details of Activities/Programs

A series of four ‘CSIRTs in Asia’ events will be organized at APAN meetings (or other big regional events if more suitable), starting with APAN45 in Singapore (March 2018) and APAN46 in Auckland (August 2018). Two events will be organized in 2019.
Each event will consist of two parts:

CSIRTs in Asia meetings
Half a day/full day meetings, where participants will be invited to give a presentation or a lightning talk on the progress of their CERT, success and failure stories and participate in discussions or debate on the most pressing security issues in the region and globally.

TRANSITS I trainings
Two-day courses, consisting of four modules aimed at new or potential CSIRT personnel, providing a solid understanding in the main aspects of working in an incident handling and response team. TRANSITS I modules:

- **Organisational** – covers how CSIRTs fit within their organisations and includes planning the team, defining its constituency, determining which services to offer, staffing, communicating with external parties, funding, and obtaining management authority.
- **Technical** – covers how intruders attack systems and their motivations, how network protocols can be abused, vulnerabilities of operating systems and services, denial-of-service attacks, hiding traces, and information gathering techniques. Includes several practical exercises.
- **Operational** – covers the incident handling process from initial reports, through triage, investigation, resolution, closure, to post-analysis. Includes practical exercises and a survey of useful tools.
- **Legal** – includes data protection, computer misuse, network monitoring, collection of evidence, and working with law enforcement agencies.

The meetings will be open to anyone who would like to attend, including members of the non-beneficiary economies and participants from other regions, seeking to increase diversity, support wider information and experience sharing and encourage networking.

Funded spots at the trainings will be offered to security staff from the NRENs of the beneficiary economies, starting from those that currently do not have a CSIRT (Afghanistan, Pakistan, Nepal, Bhutan, Cambodia and Philippines). Each time a different staff member(s) from the target NRENs will be invited to participate at the training. By the end of the project, at least one staff member from the 16 beneficiary economies will have attended the training.

3.4. Deliverables

No.	Deliverable name	*Type	**Delivery date (in months)
1	CSIRTs in Asia (meeting and training)	Capacity building event	M3 (March 2018)
2	CSIRTs in Asia (meeting and training)	Capacity building event	M8 (August 2018)
3	Report (Year 1)	Report	M12 (December 2018)
4	CSIRTs in Asia (meeting and training)	Capacity building event	M15 (March 2019)
5	CSIRTs in Asia (meeting and training)	Capacity building event	M20-21 (August-September 2019)
6	Report (Year 2)	Report	M24 (December 2019)

3.5. Milestones & Timeline

No.	Milestone name	*Due date (in month)	**Means of verification
1	Trainer volunteer contracts signed for APAN45 event	M1	Contracts
2	Call for proposals for the meeting and invitations for training participants sent out	M1	Information available on APAN45 website + individual emails
3	List of participants for the training confirmed	M2	List of participants with contact details
4	Programme for the meeting and training confirmed and announced	M2 – M3	Information available on the APAN45 website
5	Blog post written about the meeting and training	M3 – M4	Blog post available online
6	Trainer volunteer contracts signed for APAN46 event	M6	Contracts
7	Call for proposals for the meeting and invitations for training participants sent out	M6	Information available on APAN46 website + individual emails
8	List of participants for the training confirmed	M7	List of participants with contact details
9	Programme for the meeting and training confirmed and announced	M7 – M8	Information available on the APAN46 website
10	Blog post written about the meeting and training	M8 – M9	Blog post available online
11	Trainer volunteer contracts signed for APAN47 event	M13	Contracts

12	Call for proposals for the meeting and invitations for training participants sent out	M13	Information available on APAN47 website + individual emails
13	List of participants for the training confirmed	M14	List of participants with contact details
14	Programme for the meeting and training confirmed and announced	M14 – M15	Information available on the APAN47 website
15	Blog post written about the meeting and training	M15 – M16	Blog post available online
16	Trainer volunteer contracts signed for APAN48 event	M18	Contracts
17	Call for proposals for the meeting and invitations for training participants sent out	M18	Information available on APAN48 website + individual emails
18	List of participants for the training confirmed	M19	List of participants with contact details
19	Programme for the meeting and training confirmed and announced	M19 – M20	Information available on the APAN48 website
20	Blog post written about the meeting and training	M20 – M21	Blog post available online

3.6. Risk Assessment

Description of risk	Impact (L/M/H)	*Likelihood (L/M/H)	Proposed risk-mitigation measures
No trainers with required skills are available for the training	H	L	At the time of project proposal submission, a few highly experienced trainers have already expressed their willingness to lead the trainings. If some trainers are unavailable for the times of the training, a long list of others can be contacted.
Not enough participants from the beneficiary economies will be able to attend the events	M	L	Participants from the beneficiary economies will be offered financial support for attending the events.
No time slots and facilities will be available for the meetings and trainings at APAN conferences	M	L	The time slots will be requested as far in advance as possible. Should there not be time or suitable facilities at APAN conferences, events can be co-located with other relevant international events in the region.
Financial loss	L	L	The budget will be strictly monitored to make sure that all events are ran without incurring a loss.

* The likelihood is the estimated probability that the risk will materialize even after taking account of the mitigating measures put in place.

4 Resources to be committed/Budgets

- Please refer to the Appendix B for the 'Budget template' and its guidelines and fill in the template in detail as itemized. A break-down cost quotation for estimated budget will be in Euro (€).

5 Expected Impacts

5.1. Benefits to TEIN and its Community – Indicative Log-frame Matrix

Indicators	Results/Benefits	Means of verification	Assumptions
Number of NREN partners receiving training	At least 60 funded attendees from 16 beneficiary economies will attend the training + up to 40 unfunded attendees in total over two years	Sign-in sheets, testimonials (written and filmed), surveys after all events	The attendees will gain operational, organisational, legal and technical knowledge that will help them successfully fulfil CSIRT functions at their home organisations
Number of courses given	4 trainings, 4 modules each	Reports, blogs, written and filmed testimonials	Highly experienced trainers will train
Number of promotional conferences and workshops	Project updates will be given at TF-CSIRT and FIRST events (at least 4 international conferences)	Slides and recordings where possible will be provided	The results of the project will be promoted, creating wider awareness and opportunities for possible wider collaboration
Number of persons trained	At least 60 funded attendees from 16 beneficiary economies + up to 40 unfunded attendees in total	Sign-in sheets, testimonials (written and filmed), surveys after all events	The participants will benefit from the training by gaining the necessary knowledge and skills for running a successful CERT team

Number of “train-the-trainers” with network engineering expertise	At least 60 funded attendees from 16 beneficiary economies + up to 40 unfunded attendees in total	Sign-in sheets, testimonials (written and filmed), surveys after all events	The attendees will train their colleagues, passing on the knowledge and experience gained at the training. They will be asked to report (informal blogs or video testimonials) on any internal trainings that they did.

5.2. Visibility/Dissemination plan

Dissemination is planned throughout the project to provide information about the project successes and outcomes as far as possible. Firstly, we will use GÉANT social media channels, such as Facebook and Twitter. The project coordinator will provide regular updates on the blog posts, posted on the GÉANT blogs website, promoted via the PeaR newsletter (received weekly by approximately 1000 members of the international R&E community). Secondly, the trainers and the attendees will be asked to share information about the project via their communication channels. Finally, the attendees will write or film short testimonials about the benefits of the meetings and trainings that will be used to highlight the achievements and importance of the project. The project will also be promoted at international events, such as TF-CSIRT meetings, FIRST conferences and others.

5.3. Sustainability of the Activity/Program

- After the two years of the project, the trusted network of the security experts in the region will have expanded. As a result, the international information and experience sharing CSIRT meetings will continue to happen in some form – perhaps as part of the APAN conferences or other events, or as stand-alone mini-conference, hosted by one or a few economies in the region;
- Project participants will have contacts in other economies in the region that can be used in case of an international incident or crisis;
- The trainers invited to lead the course are all well-known members of the international CSIRT community. Knowing them and having their contact details will be beneficial for the participants when they need an advice or an introduction in the international security collaboration groups;
- The participants of the training will gain necessary knowledge and materials needed to train their colleagues in their home institutions.

APPENDIX A - Information on the participants A1.

CV’s of PI and his/her publication list

- Refer to section 2.

A2. Publication lists of collaborating partners/participants

- N/A.

APPENDIX B - Resources to be committed/Budget (separately distributed)

B1. Budget template

NOTICE

All personal data (such as names, address, CVs, etc.) referred to in the proposal will be used only for the evaluation process. Any comments or questions would be welcome and should be addressed to tech@teincc.org.