CSIRT collaboration in Europe

EUNITY Project Workshop

Cybersecurity and Privacy Dialogue between Europe and Japan

11-12 October 2017, Tokyo

Baiba Kaskina, TF-CSIRT Chair

Topics

- TF-CSIRT
  - Strategy
- Trusted Introducer
- CSIRT Maturity
- TRANSITS training
- NIS directive and CSIRT network
  - CEF funding
- Other cooperation groups
  - EGC
  - Regional
  - Bilateral
- Other players

TF-CSIRT

Task Force Computer Security Incident Response Teams

- Forum for exchanging experiences and knowledge in a trusted environment in order to improve cooperation and coordination
- 3 meetings a year
- Host organisation - GEANT
- All inclusive - Academic (NREN) – Governmental – Commercial
- CSIRT Services, common standards and procedures, joint initiatives
- Liaison with ENISA, FIRST, APNIC and others
- https://tf-csirt.org/
- Focus on European region (RIPE NCC service area), but not limited

TF-CSIRT – historical perspective

- Started in 2000 as mostly academic initiative
- Longest running task force at GEANT
- We just had 52nd meeting

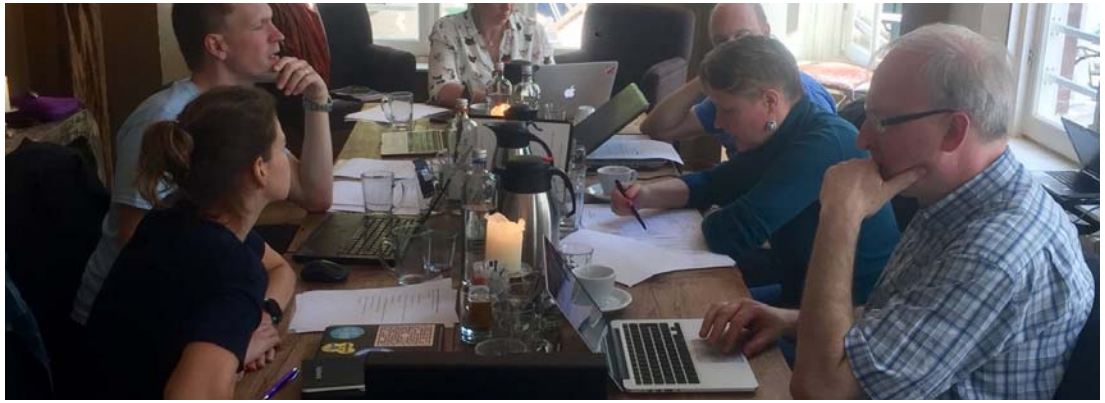
TF-CSIRT – meetings

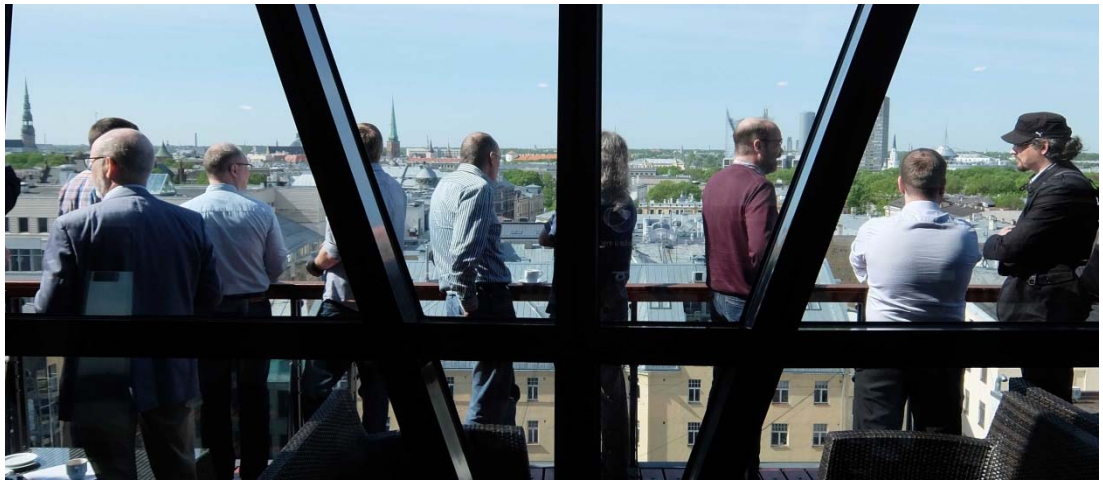
- 3 times per year
- 130 – 200 participants
- Community – 315 teams
- 2-3 days, social event
- Different location every time

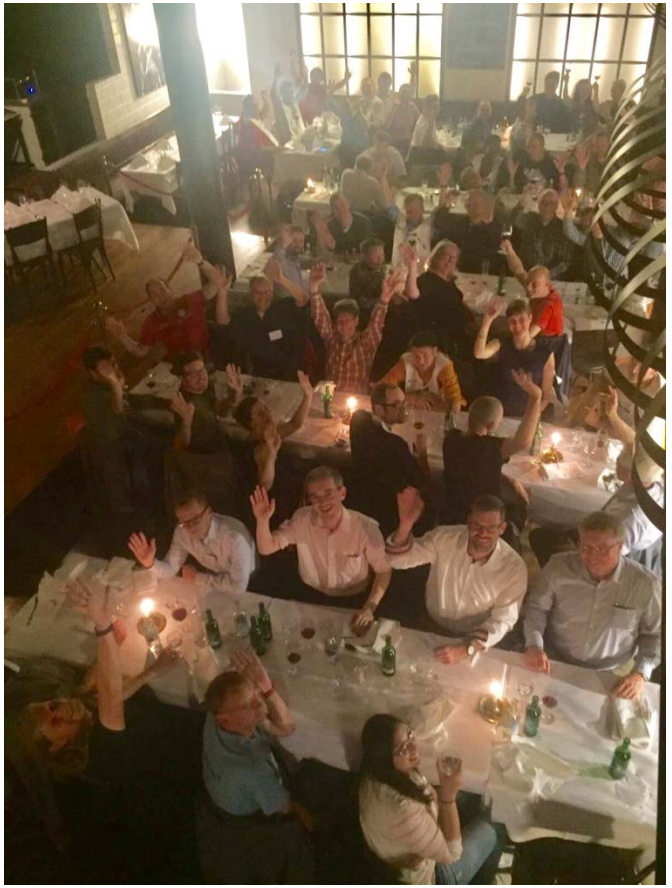
TF-CSIRT – Steering Committee

- 5 elected members from the community (including the Chair) + representative from GEANT
- Term – 2 years, can be re-elected for another 2 years
- Elections for 2 members every year
- In the future
  - Term 3 years?
  - More members – 7+1 = 8?

TF-CSIRT







TF-CSIRT Strategy

- Formulated in 2017
- Mission, critical success factors, strategic aims, goals
- Authors – TF-CSIRT SC, GEANT, TI

TF-CSIRT Mission

The mission of TF-CSIRT is to facilitate and improve the collaboration between the European CSIRT community to make cyber space a better place.

Why Us?

TF-CSIRT operates with a European mindset, and strives to make it services and meetings inclusive, accessible, easy-to-reach, and affordable for all CSIRTS in Europe – regardless of sector. Through the Trusted Introducer service, TF-CSIRT can offer well-maintained and up-to-date information and provide teams with recognition status via its differentiated listing, accreditation and certification processes.

Critical Success Factors

1. Knowledge within and outside the community is leveraged to provide high quality training and trainers.
2. Live meetings happen.
3. A governance and financial models that are fit for purpose.
4. We provide a reliable infrastructure that meets community needs.
5. We drive projects with impact.
6. There is sustainable membership development and engagement.
7. We foster the “we feeling”.
8. There are trusted information and maturity processes.
9. TF-CSIRT has prestige and visibility.

Strategic Aims

1. Improve TF-CSIRT governance.
2. Leverage community knowledge.
3. Champion the prestige and visibility of TF-CSIRT.
4. Develop a future business and financial model.
5. Improve face-to-face engagement.
6. Improve internal organizational processes.
7. Safeguard and enhance the trusted infrastructure and maturity process.

TI – Trusted Introducer Service

The trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams

- Maturity: Listing, Accreditation, Certification
- Team Directory: Public & Member access
- Closed meeting for the Accredited and Certified teams
- Open and Secure mailing lists
- Other services (member restricted)
- https://www.trusted-introducer.org/

CSIRT Maturity – 3 steps

1. Listed
2. Accredited
3. Certified

CSIRT Maturity – Listed teams

- Registration (only listed – 160 teams)
- Team exists – provides basic/substantial services
- Contact information
- Constituency
- To get listed – 2 sponsor teams needed

CSIRT Maturity – Accredited teams

- Full members of the community
- September 2017 – 155 teams
- Procedures in place
- RFC2350
- Accreditation takes 1-4 months
- Fees
  - 800 EUR/year – initial fee
  - 1200 EUR/year – annual fee

CSIRT Maturity – Certified teams

- Based in SIM3 (Security Incident Management Maturity Model) model
- SIM3 describes 45 parameters, divided over four categories: Organisation, Human, Tools, Processes
- Minimum score needs to be attained for each parameter
- 22 teams

CSIRT Maturity – why certify?

- Public Relation reasons – locally and internationally
- To evaluate CSIRT organization against international criteria
- An external drive to understand, document and put in order processes within the CSIRT team
- To establish or put in order auditing, accountability and reporting schemes
- To implement continuous improvement in a quality management framework

TRANSITS Training

CSIRT personnel training

- TRANSITS I: Operational, Organisational, Legal and Technical
- TRANSITS II: NetFlow Analysis, Forensics, Communication, CSIRT Exercises
- Over 1000 security professionals trained in Europe and more in other regions
- Knowledge exchange

NIS directive

Directive on security of network and information systems – Scope:

- National strategy on the security of network and information systems
- Cooperation Group
- CSIRTs network
- Security and notification requirements for operators of essential services and for digital service providers
- National competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems

NIS directive – CSIRT network

- Members:
  - CSIRTs
  - CERT-EU
  - Commission (observer)
  - ENISA (secretariat)
- Operational information exchange
- Discuss coordinated incident response
- Support member states in addressing cross-border incidents

CEF Funding

- "Core Service Platform" – MeliCERTes
- EU CEF framework (under SMART 2015/1089)
- Development timeframe 2017-2019
- Platform areas:
  - incident management: exchange of incident related data and security feeds
  - event management: exchange of threat/vulnerability related information
  - artefact analysis: exchange of artefact related information
  - secure communications: secure conferencing, "chat" and file sharing
  - contact management

European Government CSIRT group EGC

- Historical group
  - Austria - GovCERT Austria
  - Belgium - CERT.be
  - Denmark - CFCS-DK
  - Finland - NCSC-FI
  - France - CERT-FR
  - Germany - CERT-Bund
  - Netherlands - NCSC-NL
  - Norway - NorCERT
  - Spain - CCN-CERT
  - Sweden - CERT-SE
  - Switzerland - GovCERT.ch
  - United Kingdom - CERT-UK
  - United Kingdom - GovCertUK
  - EU institutions, agencies and bodies - CERT-EU

Other Cooperation

- Regional
  - Central European CSIRT group
  - Baltic CSIRTs
  - Nordic CSIRTs
- Bilateral

Other Players and Areas

- ENISA
- FIRST
- ITU

- Help to establish new CSIRT teams
- Training, materials
- Train the trainers
- Development of tools
- Best practices, benchmarking

Questions

Who?

What?

When?

Where?