CSIRT Network
Work Program for 2017-2022

The Work Program describes a set of goals for the CSIRT Network required in order to build a solid trusted network in which relevant information can be exchanged between all CSIRTs in accordance with art. 12 of the Directive.

As the CSIRT Network success depends on several factors the current document is divided in to four elements, preparatory work, as well as short, mid and long term goals. Preparatory tasks consist of fundamental requirements for a successful launch of the CSIRT Network in February 2017. Short-, mid-, and long-term goals on the other hand define tasks for each of the three reporting terms. Importantly the set of tasks for each reporting period needs to be seen as a non binding guideline that needs additional specification and continuous adjustment.

Preparatory Work (2016 – 2017)

Governance

By 9 February 2017 MS shall ensure appropriate representation in the CSIRT Network[1].

- Collect a maximum of three national standing representatives as members of the network (two standing and one alternate)[2] for the period 2017-2022.

Discuss the internal contact directory for CSIRT Network – ENISA, TI hosted

- Reach decision on whether to reuse an existing one or create a new one.

Finalise internal organizational structure.

- Adopt the Terms of Reference / Rules of Procedure.

Develop an annual and multi annual work plan and define preliminary goals to be reached.

- Adopt the Work Plan.

Decide on and approve number of physical meetings per year (e.g. three plenary meetings per year; one at least co-located with another CSIRT event in Europe e.g. TF-CSIRT in May; one at least as a stand-alone event).

Define upon practical means of communication

- Operational exchange channels may consist of e.g.
  - Open mailing lists for adequate communication (e.g. CSIRT Network representatives for administrative exchange, working groups, team lead and open operational exchange) – ENISA/listserv, TI hosted mailing list
  - Conference call facility – ENISA/adobe connect facility, individual facilities by MS

1 Quote from NIS Directive/Article 24 Transitional measures

2 Quote from the to be agreed ToR/RoP document

- Confidential exchange mechanisms via mail[3], chat, web portal) – ENISA/CSIRT Network portal, TI hosted encrypted mailing list (crypto remailer)

- *Discuss specific security requirements for operational services (e.g. exchange portal).*
- *Discuss the requirement for operational procedures – ENISA/Cyber-SOPs*

Define adequate CSIRT maturity levels for the Network[4] (comparable to e.g. FIRST[5], SIM3 certification; baseline capabilities by ENISA[6]; current maturity project).

Short Term Goals (February 2017 – August 2018)

"Developing trust and confidence between CSIRTs"

CSIRTs reach a first maturity level based on the agreed maturity measurement schemes for CSIRT Network

Strategic objectives:

- Approve the annual and multi-annual Work Program
- Approve ToR and RoP
- Define CSIRT Network support service needs (document translation service, trainings, exercises, development of specific good practice guidance on…)
- Define Operational Procedures for the CSIRT Network
- Connecting Europe Facilities - Influence the Cybersecurity DSI project by forming relevant working groups, identify and agree upon benefits (joined position)
- Build functional exchange with the Cooperation Group (based on ToR)
- Prepare first evaluation report for the Cooperation Group.
- Revise the Work Plan as needed (e.g. roadmap and goals for the mid-term)

Operational objectives:

Establishment of an internal contact directory for CSIRT Network

- Create and maintain public web portal for the CSIRT Network ("virtual CSIRT Network portal" that includes contact details for the Network's Chair / members and links to the members' individual websites).
- Create and maintain a preliminary private web portal and collaboration space (implementation of the Work Program).

Basic Information Exchange

- Adopt TLP based approach for information exchange of non-classified information concerning individual incidents (e.g. specific versioin of TLP-Amber).
- Discuss lessons-learnt from exercises in relation to the support to cross-border security incidents of network and information systems, including ENISA's Cyber Europe series.

---

3 In order to enable seamless & secure exchange of sensitive information cryptographic mailing list (remailer) with standardised key-management processes would be the preferred solution.

4 Cross certification is not intended, the maturity level should rather be based on individual assessment based on an agreed common criteria set.

5 The groups mentioned here are to act as role-models. There is no need for a 1:1 transposition. The purpose is to visualise the intended level of maturity.

6 https://www.enisa.europa.eu/topics/national-csirt-network/csirt-capabilities/baseline-capabilities

- Exchange information on CSIRT services, operations and cooperation capabilities.[7]
- Exchange information on CSIRT trainings, exchange program for teams and other capacity building efforts.
- Exchange special information (individual documents relevant for other nations like: case-studies, English language good practice papers, IOCs). See 7 for further details.

Tactical objectives:

Team Descriptions (first stocktaking)

- Establishment of an internal contact directory for members of the CSIRT Network.
- Teams conduct maturity self-assessment.
- Create an overview about the teams' provided services[8], individual maturity levels and details about service times, freedom of information act legislation etc. (possibly based on existing team service descriptions like RFC2350, via TI, FIRST, or existing ENISA information).
- Maintain an overview in a central location, e.g. a closed segment of the CSIRT Network portal.

Mutual Assistance - Voluntary buddy/mentor-model

- Building upon initial maturity stocktaking overview
- Optional for teams who want to increase their maturity (in addition to the existing ENISA support)
- Define training needs for CSIRT Network members (e.g. specification for CII sectors)

Trust Building

- Contribute to the preparatory work for CSIRT Network exercise (as a key element of the preparation for Cyber Europe 2018)
- Organise a team building event
- Regular meetings (plenary and, if decided, special interest groups and expert workshops)

Overall Success Factors:

- At least 50% of teams reach a first level of maturity
- Adopt terms of reference and operating procedures for the CSIRT Network
- Adopt multi-annual work program for the CSIRT Network
- Contact Directory is established and regularly updated (at a minimum three reviews per year - possibly linked to the meetings / through CSIRT self maintenance)
- Countries have joined the CSIRT Network with appropriate representatives
    - Regular representatives and proxy was named by each MS (according to ToR)
    - Attendance rate during meetings
- Information exchange has started (each team shares 5 documents - see 7 for

7 Formalised team presentations that describe the teams' character, the essential services, and the capabilities that differentiate this specific CSIRT from other teams.

8 Security Incident Response Teams (SIRTs) Services Framework Version 1.0 http://www.first.org/_assets/global/FIRST_SIRT_Services_Framework_Version1.0.pdf

further details)
- At least one team building event has been conducted
- Regular communication checks conducted based on an agreed interval

Mid Term Goals (August 2018 – March 2020)

"Improve EU-wide preparedness"

*CSIRTs reach a second maturity level b*ased on the agreed maturity measurement schemes for the CSIRT Network.

Strategic objectives:

- Review of short term KPIs
- Revise the multi-annual work plan if needed (roadmap and goals to be reached in the long term)
- Review ENISA's role and tasks according to the group's needs and overall tasks delegated by the NIS directive (appropriate resources reserved as part of ENISA's annual work program and allocation based on justified needs by the CSIRT Network?)
- Review and finalize first evaluation report for the Cooperation Group (report to be submitted on 9 August 2018).
- Prepare second evaluation report for the Cooperation Group (report to submit on 9 March 2020)
- Define rules of procedure for visitors in order to allow their participation in the CSIRT Network

Operational objectives:

Maintenance of an internal contact directory for the CSIRT Network

- Define the scope of provided contact data, its format, retention and storage policy, as well as guidelines.
- Conduct regular communication checks.
- Define update procedure & com-check procedure

Information Exchange

- Exchange and discuss non-commercially sensitive information related to specific incidents and associated risks at request of a MS
- Exchange and make available non-confidential information concerning individual incidents on a voluntary basis
- Exercise coordinated response to cross-border incidents (possible under the Cyber Europe exercise series or EU SOPs exercise)
- Connecting Europe Facilities – establishment of appropriate representation channels for CSIRTs (e.g. successful integration into the governance mechanisms) on aspects of operational information sharing

Tactical objectives:

Team Descriptions

- Teams conduct next level of maturity self-assessment

Mutual Assistance - Voluntary model

- Define Processes (e.g. cooperation mechanisms, contact management and maintenance, escalation...) in addressing cross-border incidents

Trust Building

- Workshops on special topics and/or trainings (e.g. 2-3 topics tbd.,)
- Form specific working groups (e.g. specific threats, joint tool development)
- Further adopt cyber exercises and training curriculum to the needs of the CSIRT Network
- Continue with annual trust building activities
- Teams promote their level of maturity
- Continue mutual-assistance support on voluntary basis

Overall Success Factors:

- 100% of teams reached the first level of maturity
- At least 50% of teams reached the second level of maturity
- High attendance rate and stable representation during meetings
- Information exchange matures (incident related information exchanged, teams continue to share documents and other special information)
- Agreed communication tools are working and are commonly used by members of the CSIRT Network to share information (acceptance rate)
- Other support tools are being extended via cooperation in working groups
- At least one additional team building event has been conducted
- 50% of the trust-building measures described in the ENISA documents[9] were „tested on“ / tried by the group
- Communication checks conducted based on agreed directory (increase of success rate)
- Active information exchange in the Core Platform
- Participation in Cyber Europe series

Long Term Goals (March 2020 – September 2021)

„Promote swift and effective operational cooperation“

CSIRTs reach third maturity level based on agreed maturity measurement schemes for the CSIRT Network.

Strategic objectives:

- Review mid-term KPIs
- Revise the current and develop appropriate new action plan (roadmap) and multi-

9 ENISA: "Scalable and Accepted Methods for Trust Building in Operational Communities" and "Good Practice Guide Network Security Information Exchanges".

annual work program (2023-2028)

- Review and finalise second evaluation report for the Cooperation Group (report to submit on 9 March 2020). This report shall serve as an input for the Commission's review of the functioning of the Directive – this report shall be submitted by 9 May 2021.
- Prepare third evaluation report for the Cooperation Group (report to submit on 9 September 2021)

Operational objectives:

Information Exchange

- Discuss lessons-learnt from exercises in relation to the security of network and information systems, including ENISA Cyber Europe series and EU SOPs exercise and update necessary procedures relevant to CSIRTs operations
- Define more advanced methods of communication and information exchange
- Improve exchange and make available non-confidential information concerning individual incidents on a voluntary basis
- Connecting Europe Facilities – CSIRTs continue to use the CSIRT Network's representation channels in order to reach enhanced operational information sharing mechanisms

Tactical objectives:

Team Descriptions

- Run teams' maturity self-assessment

Mutual assistance

- Identify further forms of operational cooperation in relation to risks and incidents
- Review and further explore principles and modalities for coordination when MS respond to cross-border incidents
- Conduct Com-checks

Continue with trust building measures

- Regular workshops on special topics and tailored trainings
- Further adopt EU cyber exercises and trainings curriculum to the needs of the CSIRT Network
- Conduct additional team building events (at least one per year)
- Visitors are invited to the meetings to contribute to the discussion on specific topics

Overall Success Factors:

- 100% of teams reached the second level of maturity
- At least 50% of teams reached the third level of maturity
- Very high attendance rate and stable representation during meetings
- Matured information exchange (e.g. information release process included as part of the teams' daily routine, each team contributes another 5 inputs; documents, special information, IoC, etc.)
- Additional communication tools are working and are broadly used in the CSIRT Network to share information; usage of a more advanced system (for instance, CEF

Platform or alternative tools and systems)
- Support tools are being extended via continued cooperation in working groups
- At least one team building event has been conducted per year
- Com-checks conducted based on agreed directory (increase of success rate)
- Active use of Core Platform for operational information sharing

Additional quick wins

Five Documents- Information Sharing

The general idea is that every MS ideally provides „5“ documents (e.g. good practice documents, concepts, special topic advisories, briefings or policies) to the group (via ENISA as the secretariat) in order to be shared on a common document repository. In order to provide full benefit the specific documents should be shared in English[10] but may be beneficial in their original language as well. The documents could be made available on a non public part of the used portal (e.g. the ENISA portal) where the Secretariat may organize in a suitable way.

By doing so the CSIRT Network builds an existing information pool that members can draw from while producing new products. As there will always be an overlap of topics, e.g. several DDoS protection documents, this process may reduce the overhead and return more complete advise in the end. Additional value can be derived from ENISA (in its secretariat role) using the provided input in order to compile joint documents / reports on special topics (after a release process including contributing authors). The outcome could then be shared publicly.

Why „5“ documents?
- Five contributions seem to be a reasonable number to be handled by each team.
- One document needs to be considered the absolute minimum, between two and may be considered acceptable, more than five documents would be highly appreciated (especially from teams with English as a first language), and ten submissions would be very much to demand (as most MS will need to go through the painful process of translation without an existing service).

Take a look into the „Venice-Files“

Translation Services

As a minimum the CSIRTs need service integration for document translation in order to allow teams to use EU-translation mechanisms. Make use of existing e-Translation building block via the Connecting Europe Facility Cybersecurity project.
Overcome language barriers of native language documents to be shared with the

10 English language documents can easily be reused. They could potentially be directly redistributed. Maturity of translation should ideally be marked („automated“, „manually refined“, „checked by native speaker & technical expert“).

group also on short notice.

Teambuilding Exercise

Italian suggestion, comparable to kick-off meet & greet in Den Haag (small groups discuss and mix in various settings), additional first thoughts available in NL and DE for such an exercise.