CSIRT Maturity Kit

A step-by-step guide towards enhancing CSIRT Maturity

8 April 2015

National Cyber Security Centre, The Netherlands
info@ncsc.nl

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Maturity is an indication of how well an organisation governs, documents, performs and measures its activities. For instance, what are the steps taken to perform a certain service? Are these steps written down? What are the different roles of the team members? Are these well-defined? How is performance measured? Is it measured regularly?

CSIRT maturity is, in turn, an indication of how well a team governs, documents, performs and measures the CSIRT services. Is the CSIRT aware of the various processes and the required steps? Are these written down, shared, examined and improved? Is it clear what the CSIRT authority and accountability is? Are there mechanisms to ensure that the CSIRT follows the formal processes and adequately serves its constituency? Are there mechanisms in place to constantly learn and improve?

The purpose of this **CSIRT Maturity Kit** is to help emerging and existing Computer Security Response Teams (CSIRTs) to increase their maturity level. This is achieved by offering a set of best practices that cover CSIRT governance, organisation and operations. The document that is presented now provides a starting point to guide CSIRTs through this process and serves as a basis for further international discussion on this topic and the exchange of best practices, in the International One Conference 2015, the GCCS2015 and the Global Forum on Cyber Expertise/CSIRT Maturity Initiative.

This document identifies, and offers suggestions for improving, 5 areas of CSIRT maturity:

1. **Foundation** – Creating and laying the foundation of your CSIRT.
2. **Organisation** – Creating internal structures and joining the right networks.
3. **Human** – Selecting and developing the most important asset of your team.
4. **Tools** – Selecting and developing appropriate automation and infrastructure.
5. **Processes** – Identifying and formalising the core services of your CSIRT.

The cyber threat landscape is constantly changing and the responsibility to prevent, detect and respond to incidents is ever more challenging. To remain effective and meet these challenges, we must focus on **capacity building**, assisting others and exchanging knowledge. This not only benefits an individual CSIRT, but also **benefits the entire community**. If individual countries have the capacity to effectively address threats in the digital domain, then countries can collectively improve the quality of cooperation. Cyber security is a **shared responsibility** and requires a **joint effort**.

Under the banner of capacity building, we must focus on increasing the **maturity level** of our CSIRTs. These teams must evolve, and sometimes grow, to deal with the new challenges we face. Only when a team is strong, can it offer help to other teams. The CSIRT Maturity Kit guides CSIRTs through this process.

ACKNOWLEDGEMENTS

For the realisation of this CSIRT Maturity Kit we would like to extend our gratitude to the CSIRT community for sharing their best practices, without which this document would not have been possible. Furthermore we want to give our special thanks to the international review committee for their valuable advice and support along the way.

PURPOSE

The purpose of this CSIRT Maturity Kit is to help emerging and existing Computer Security Incident Response Teams (CSIRTs) to increase their maturity level quickly and effectively by bringing them in touch with a specific set of best practices that cover the main areas of governance, organisation and operations of a CSIRT. These best practices are either referenced or provided directly as part of the Kit and are placed in a logical context, with additional explanations and advice wherever useful and possible.

Thus, the CSIRT Maturity Kit, is a practical, hands-on document that can be directly applied by experienced and inexperienced CSIRT professionals alike. The Kit is written in such a way as to help them navigate the vast range of possibilities for establishing or enhancing a CSIRT.

Many choices have been made on content, by the authors, in consultation with an international review committee. Therefore, it is important to note that other ways of doing things may be just as successful, and that other references or best practices can be used. In fact, collaboration with other maturity related efforts in the world will be an on-going effort.

This Kit is not the last word in CSIRT matters, but rather an outreach to actually help teams increase their maturity efficiently. It is a living document that will be regularly updated with new information when this becomes available, particularly after the ONE Conference and the Global Conference on Cyber Space GCCS2015.

TARGET AUDIENCE

The primary target audience of this CSIRT Maturity Kit is national, critical infrastructure, corporate, research & education, and governmental CSIRTs worldwide. This kit will be especially useful for recently created teams and teams who have not yet had the opportunity to consciously improve their maturity level.

The subject matter of this kit is such, that we can safely recommend its use to all substantially sized CSIRTs in all areas of society. We believe it will be beneficial to both novice and experienced teams.

1 FOUNDATION

This chapter describes how to lay the foundation for your CSIRT[1]. This includes the various steps you should follow to create a new team, such as developing a business plan, assessing the relevant legal frameworks and clearly identifying your constituency. Furthermore, this section introduces the concept of CSIRT maturity and its vital role in the building a sturdy foundation for your team.

1.1 CSIRT creation

The European Union Agency for Network and Information Security (ENISA)[2] provides a wealth of documentation to assist CSIRTs. Included in this documentation is *"A Step-by-Step Approach on How to Set Up a CSIRT"* [3]. This document offers a well-structured approach to setting up a CSIRT and is available in 26 languages, including English, Spanish, Chinese, Hindi and Russian.

An alternative, action-plan oriented approach to setting up a CSIRT is offered in: http://www.cert.org/incident-management/csirt-development/action-list.cfm

1.2 CSIRT business plan

What is the reason behind your decision to create a CSIRT? You need to establish this very clearly. This needs to be more than only a formal decision – you must be able to easily explain it in speech and in writing. Formulate this into your "business plan", which could also be part of e.g. a (national) cyber security strategy.

The business plan should address how to gain support for your CSIRT. This means that you at least:

i. See how your CSIRT fits into your parent organisation's cyber security strategy, whether that's a commercial or not-for-profit organisation, a government, or a state.
ii. Identify the stakeholders to cooperate with and/or to convince –and define a strategy and tactics for how to achieve this.
iii. Identify the relevant cultural issues that come into play to make your CSIRT into a success – and plan how to turn those challenges into opportunities.

Some interesting examples of relevant national strategies:

- New Zealand: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf
- Japan: http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf
- The Netherlands: https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html

[1] The term "CSIRT" meaning "Computer Security Incident Response Team" is a commonly used term. The term "CERT" is as common, however we avoid this in this Kit as this is a trademark of Carnegie Mellon University, home of CERT/CC.
[2] More information available at: http://www.enisa.europa.eu/
[3] Available online at: http://www.enisa.europa.eu/activities/cert/support/guide

1.3 Measuring CSIRT Maturity

A useful tool for measuring CSIRT maturity is the Security Incident Management Maturity Model (SIM3). This model identifies 40+ parameters that measure four categories of maturity: Organisation, Human, Tools and Processes. For each category, the SIM3 approach enables you to assess and subsequently increase the overall maturity of your CSIRT. You find the most recent version of SIM3 here:
https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

SIM3 has been used to assess and certify teams of all kinds inside Europe: national, government, corporate, research and other teams. The certification uses a parameter profile with minimum demands for each parameter. This is provided here for your reference:
https://www.trusted-introducer.org/TI-Certification-Profile.pdf
However, we recommend that you adapt the reference profile to your own needs, setting the priorities that are important for **your** team. If you want your team to be certified by the European CSIRT community, you can find more information on https://www.trusted-introducer.org/processes/certification.html.

An especially important pre-requisite of CSIRT maturity is support from your organisation's management. For effectively building up your CSIRT maturity level it is essential that your CSIRT has active management support. This means that your team has to be part of the governance and auditing in your organisation, as is referred to in the highest maturity level in the SIM3 model. We strongly recommend that you make sure that at least the following aspects of your CSIRT are at this level 4, meaning they are audited by at least one management layer higher than your CSIRT leadership:

- CSIRT Charter (see 2.2 below)
- CSIRT service & service level description (can also be part of your Charter)
- CSIRT reporting & auditing process (can also be part of your Charter)

You need these essential aspects to be supported and audited by the management of your organisation because the CSIRT primarily serves the interests of your organisation or constituency as a whole. The CSIRT protects the primary/business process, the organisation's reputation and all supporting processes. For example, in the case of a CIIP[4] CSIRT that translates into protecting the critical information infrastructure of a country. Therefore the highest form of governance in an organisation needs to take responsibility for the CSIRT and stimulate and support it. This must be reflected in governance, reporting and auditing.

Specifically for national/governmental CSIRTs ENISA has a series of "baseline capabilities" documents at http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities .

1.4 Addressing legal constraints

Most CSIRTs will be directly or indirectly involved in the protection of fundamental legal constraints, like for instance:

- Data protection
- Healthcare non-public personal information protection
- Civil liberties
- Privacy

[4] CIIP: Critical Information Infrastructure Protection

You need to assess the legal framework that applies to these topics in your country and see how it impacts your work. It is important to clearly understand how you must contribute, or can be expected to contribute to the protection of such issues. We recommend that you write this down into a policy document and train your staff accordingly.

1.5 Case studies

For an important part, increasing CSIRT maturity can be achieved through the adoption of best practices that have been documented by other teams. It is likely that they have gone through similar experiences and difficulties in the establishment and fine-tuning of their team. Therefore, we recommend reading the following case studies:

- This document illustrates the growth and evolution of the European CSIRT community in general and the Dutch National CSIRT in particular. "A Dutch Approach to Cybersecurity through Participation" (Clark, Stikvoort, Stofbergen, Vd Heuvel; IEEE Sep/Oct 2014)
- This document provides interesting case studies of the Columbian and Tunisian govCERTs and on creating a Financial CSIRT: http://www.cert.org/incident-management/publications/case-studies/index.cfm

2 ORGANISATION

It is crucial for the success of your CSIRT that it is well-defined, well-organised, part of the governance and auditing of your organisation, and that it connects with the CSIRT community in your country and worldwide. This section surveys some essential features in this regard.

2.1 CSIRT Services

You need to define the services that your CSIRT will offer. A good starting point for that assessment is the CERT/CC list of services, which has also been adopted by e.g. ENISA: https://www.cert.org/incident-management/services.cfm

We strongly recommend that you limit yourself in your choice of services. Trustworthiness and reliability are essential qualities for your CSIRT, and this means that it is better to excel in the reliable performance of a few crucial services, than to have a wide range of services with lower performance. Make absolutely sure that you can fulfil the demands of your basic services!

2.2 Charter (Organisational Framework)

We strongly recommend that you write a Charter or Organisational Framework for your CSIRT as an internal document and, furthermore, that you get it approved by the highest available management/governance layers in your organisation. Time and again[5] this proves to be one of the most effective ways to anchor your team in the organisation. It ensures that you have the proper authority to do your work right and that working escalation procedures are in place. In addition, it guarantees that your team is being regularly audited, which helps you raise awareness and funding to keep improving your CSIRT. We advise you to address at

[5] This has been the experience in the certification of 15 European CSIRTs and in audits and assessments of various other teams.

least the following topics in your CSIRT's Charter (most of these are explained in SIM3, see 1.2):

- Mandate: an official decision (or law) enabling your CSIRT
- Constituency: the group(s) that your CSIRT aims its services at (your clients)
- Authority: the extent to which your CSIRT is allowed to take action in regards to your constituency
- Responsibility: the extent to which concern and action are required and expected of your CSIRT
- Service description: which services does your CSIRT provide towards its constituency
- Service level description: what kind of service levels can your constituents (and others) expect of your CSIRT
- Outreach to constituency: in what ways do you communicate with your constituency, and how do you stay in touch (including visits, seminars, conferences, magazine)
- Participation in existing CSIRT frameworks
- Acceptable Use Policy (AUP) and Security policy (in both cases referral only, do not include in Charter: also see 5.7)
- Organisation of your team, including:
    - Organisation chart and functions
    - Staff education policy
    - Meeting process
    - Main tools (incident database, e-mail, phone: including aspects of resiliency)
- Internal escalations to:
    - Governance/board level
    - Press/communication office
    - Legal office
- Reporting process
- Audit/feedback process (the link to the governance level)

This document may serve as an example:
https://www.ncsc.nl/binaries/content/documents/ncsc-nl/organisatie/wat-is-het-ncsc/operational-framework/1/Operational%2BFramework%2B2_0%2BNCSC%2BNL.pdf

While the Charter is an **internal** document for your team, you also need to publish a public description of your team online. We advise that you use rfc-2350 , which is the existing international standard designed for exactly that purpose:
http://www.ietf.org/rfc/rfc2350.txt

Examples of filled-out rfc-2350s:

- DFN-CERT, Germany: https://www.dfn-cert.de/en/rfc2350.html
- ID-CERT, Indonesia: http://www.cert.or.id/rfc/en/

Additionally, we advise you to take into consideration making a special webpage for your CSIRT. This could be for example 'www.yourcsirt.tld'. If you service a single organisation you could make a "slash security page" for your organisation on the public website. For instance, if your organisation's domain name is mydomain.tld, then your slash security page would be:
https://www.mydomain.tld/security

When creating this site, please consider the following advice:

- Accessing the site via **http://** should automatically redirect to a secured **https://** connection.

- Your version of rfc-2350 should be available from your webpage or slash security page, together with any other relevant public information about information security regarding your organisation.
- Make sure that your webpages and rfc-2350 are available **in English**, in addition to your local language(s) and any other language that is important to you. English is the common language of the worldwide CSIRT community.

2.3 Incident Classification

Establish an incident classification scheme or taxonomy. This helps you in explaining what your team is working on both to your constituency and when reporting within your governance structure. It will help you focus and set priorities.

The best thing to do is to use a classification scheme that is used by more teams in your country or region. This way you can compare statistics and keep a better eye on the current trends together with other teams.

A good and useful example of such a taxonomy is one that is popular in Europe among CSIRTs: https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Another useful classification can be found in this document by FIRST: https://www.first.org/_assets/resources/guides/csirt_case_classification.html

2.4 National and international co-operation

Make sure that you address/discuss the following areas of co-operation. Even if these do not fall within the mandate of your CSIRT, it is in your organisation's and indeed your country's interest to stimulate all these to be covered by you and/or other teams:

2.4.1 National CSIRT point of contact

Your country must have a national point of contact where Internet-related security incidents can be reported, especially for cases where it is not clear which CSIRT to report to. Ideally, this is the national CSIRT, but if this has not yet been established this role could be fulfilled by one of the teams in your country which agrees to act as CSIRT-of-last-resort. The fact that a team is a national point of contact does not necessarily mean that it will handle all reported incidents, it may also choose to only co-ordinate such incidents – or to simply refer them to the appropriate CSIRT without co-ordination. The question of which CSIRT will respond to and coordinate an incident depends on the authority and available resources of that specific team

Examples of national CSIRT points of contact are:

- CERT.br in Brazil: http://www.cert.br/en/
- CERT.at in Austria: http://cert.at/index_en.html

2.4.2 Co-operation with law enforcement

Get in touch with the cyber crime experts or department of your national law enforcement agency. Start a co-operation with them as there is mutual benefit in that. The cyber crime "cops" need your inside knowledge of real cyber crime cases – and you want a good working relationship with them for the case of prosecutions which involve operations or expertise of your team.

ENISA has at least two useful training exercises available in this area on http://www.enisa.europa.eu/activities/cert/training/training-resources/legal-cooperation:

- Cooperation with Law Enforcement agencies
- Cooperation in the Area of Cybercrime

Additionally, ENISA has launched a useful guide for incident responders, with a special emphasis in evidence gathering and the cooperation with law enforcement: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/electronic-evidence-a-basic-guide-for-first-responders

2.4.3 National CSIRT cooperation

Make sure to join your country's national CSIRT cooperation platform, or set that up if it does not exist yet. In many countries such a cooperation platform has been proven to be very beneficial for establishing trust relationships between the teams, for handling actual incidents and to learn from each other. Examples can be found on: http://www.enisa.europa.eu/activities/cert/background/coop/past-present/national-cooperation .

2.4.4 Sectoral cooperation

Assess whether any cooperation exists on CSIRT-level in the sector (government, finance, healthcare, education/research, etc.) your CSIRT is located in. For example, national/government CSIRTs cooperate in the EGC Group: http://www.egc-group.org/index.html. If such a cooperation platform exists, consult with them to find out the benefits and responsibilities that come along with joining them. Other examples of CSIRT cooperation platforms: http://www.enisa.europa.eu/activities/cert/background/coop/past-present/international-coop/sector-coop.

ISACs (Information Sharing and Analysis Centers) are also worth considering as a model. See e.g. http://www.isaccouncil.org/memberisacs.html

2.4.5 Transnational cooperation

We strongly advise you to join a transnational CSIRT cooperation platform that is relevant for your team. This is not always possible because some have more limited scopes than others, but we urge you to explore the possibilities. Such transnational cooperation platforms have been essential in the development of the CSIRT community ever since 1993. Most of them also provide some form of CSIRT training. The most prominent examples of such co-operations:

- Africa: AfricaCERT (http://www.africacert.org/home/)
- Asia-Pacific: APCERT (http://www.apcert.org)
- Europe: TF-CSIRT (https://www.terena.org/activities/tf-csirt/) and Trusted Introducer (https://www.trusted-introducer.org): the Trusted Introducer provides the trust infrastructure for the TF-CSIRT community
- The Americas: OAS Cyber Security program (https://www.sites.oas.org/cyber/en/pages/default.aspx)
- Latin-America: LACNIC AMPARO (http://www.proyectoamparo.net/en)
- National CSIRTs annual meeting: this is a very successful project of CERT/CC bringing together national CSIRTs worldwide. See e.g. http://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

2.4.6 Worldwide co-operation

We advise you to seriously consider becoming a member of the worldwide forum for CSIRTs, the Forum of Incident Response and Security Teams (FIRST): http://www.first.org. All

transnational cooperation platforms referred to above are connected to FIRST. This forum has become too large to perform actual incident handling activities, but it is an extremely valuable resource for connecting with other teams from all CSIRT communities worldwide, including the vendor community. This can help you acquire contacts for incident/threat handling, and it allows you to join projects, trainings and useful initiatives for your team. Finally, FIRST organizes a conference each year, which is a good place to network in the CSIRT community.

On the global telecommunication level, the ITU is strongly committed to advancing cyber security. This includes CSIRT development programs. For the ITU Global Cybersecurity Agenda (GCA) see http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

3 HUMAN ASPECTS

The most important assets of your team are your team's members. CSIRT work is not standard, run-of-the-mill work. It is highly specialised work, done in a challenging environment and often under time pressure. Finding the right people for your team, training them well and keeping them for at least a number of years for maximum efficiency is crucial to the success of your CSIRT. This section discusses some of the most important aspects in this area.

3.1 Code of Conduct/Practice/Ethics

It is important that the members of your CSIRT share the same understanding of what a CSIRT professional can do and what is not allowed, not right, or not ethical. There will be differences in this set of expectations between CSIRTs – therefore it is important to establish your own Code of Conduct, and even more importantly: discuss this inside your team on a regular basis. Your team needs to understand that the ethics are fundamental to the CSIRT community: examples are the confidential handling of information entrusted to you; spreading sensitive information only on a need-to-know basis; and not rushing to publish vulnerabilities but giving stakeholders (e.g. vendors) a reasonable chance to correct them first.

This document can be used as an example of a good Code of Conduct:
https://www.trusted-introducer.org/CCoPv21.pdf
This Code of Practice is supported by many European CSIRTs.

3.2 Personal Resilience

Personal resilience is mainly an issue for smaller CSIRTs which have a small constituency and/or a low number of security incidents. Such teams face the choice whether to appoint 1 or 2 fulltime professionals for the CSIRT work, or to work with a bigger number of team members who do their CSIRT work on a part-time basis and perform other functions in the same organization.

The rule of thumb is that a CSIRT needs **at least** 3 team members to function, but it is preferable to have a team consisting of 5 members or more. The reason for this is resilience: with 3 team members, one can be on leave and another one can have the flu, which still leaves one team member to cover the basic functions of the CSIRT. It is fine if such team members work part-time on their CSIRT activities, as long as there is (formal) agreement that when a big incident occurs, they will devote all their time to solving that incident. :The CSIRT task takes priority in the case of urgent incidents.

A possible compromise solution for a smaller team is to appoint 2 fulltime team members – and add 3 or 4 part-time members.

Bigger teams, with 7 or more fulltime members, face personal resilience issues too. Such teams usually perform more services, and work with sub-teams. That means that personal resilience stays an issue to be addressed especially within the highest priority services. For this reason it can prove beneficial to ensure that team members can work in more than one service area.

3.3 Skillset Description

Universities and schools do not train CSIRT professionals (yet). The CSIRT work is not mainstream. For most CSIRTs it is hard to very hard to find good professionals. You should at least be aware of what kind of people you are looking for and what kind of skills they need to have. For the skillset there exists an excellent write-up:
https://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm

You will need this skillset for the hiring campaign, for job interviews – and also for establishing where your candidates will need extra training. You need to take this into account right from the start: additional training will be necessary in almost all cases (see 3.4).

3.4 Training (Schooling and education)

Ongoing professional training is essential for all your team members to keep up with new attacks and mitigation techniques. As already argued in 3.3 you will need to provide for a training framework for your CSIRT. We recommend that you write a "personal development plan" for each team member, together with that person. Such a plan allows you to make sure that your team members follow a minimum set of required trainings – plus it opens the possibility for them to take more advanced courses and for the team management to track that. A good way of managing this is to allocate an annual training budget for your team members.

You should have/allow at least the following trainings:

i. Internal training: to get new team members up to speed. We advise to write down what the program and contents of such a training are (a team wiki is a great tool to do so), and to have at least 2 people in charge of giving internal training.

ii. External technical training: to make sure that your team members can gain the technical knowledge they need to do their job and to help your team gain or maintain the leading position that a CSIRT needs to have in regard security matters .

iii. External communication/presentation training: communication and presentation skills, both written and oral, are essential to the CSIRT profession. Depending on the specific job that a team member has, there will be more or less emphasis on interpersonal communication, however in general these skills are very important. Allow your team members to train in these areas.

iv. Incident drills: invest in incident drills, which are real-time group exercises, simulating threats and incidents. You can do this inside your team, to test how effective your team is, how well the procedures work, if the available skills are sufficient, etcetera. You can also do this together with other teams. In some sectors such drills are already being organized: participate, if you can. Warning: it is a lot of work setting up and running

incident drills. Use existing scenarios if you can. A good starting point is the ENISA training material referenced below.

v. Training through conference/workshop attendance. Encourage your team members to attend relevant conferences or workshops – and to participate in fora or working groups that will both increase the expertise level of your team members and contribute to the knowledge level of your CSIRT as a whole.

The following is a list of reputable CSIRT (related) training groups or training providers. Author and reviewers know these from experience and reflect favourably on them. Although the list is not exhaustive, it can provide you with a good start:

- Operating worldwide, FIRST (see 2.4.6) has an Education Committee which aims to promote CSIRT training worldwide, and which supports initiatives in this field: see http://www.first.org/about/organization/committees#edc. FIRST regularly supports TRANSITS trainings (see below) and is working on a new body of basis CSIRT training materials, expected to be available starting mid 2015. FIRST also regularly organises train-the-trainer sessions.
- TRANSITS is an introductory 2-3 days CSIRT training course[6], developed in Europe but popular all over the world. TRANSITS is a not-for-profit framework aimed at making trainings available to as many CSIRT team members as possible. Therefore you can use the materials at very low cost, as long as you can demonstrate a good quality plan for the training. All details see: https://www.terena.org/activities/transits/
- Transnational CSIRT fora: most transnational CSIRT cooperation platforms, mentioned in 2.4.5, are active in promoting and improving CSIRT education and training. For instance, TF-CSIRT fosters the TRANSITS framework and ensures that the materials are being updated regularly. TF-CSIRT also organises train-the-trainer sessions.
- ENISA. Although ENISA's remit is the EU and they focus on national/governmental CSIRTs, their website is an invaluable resource for CSIRT related materials – and for CSIRT trainings. We highly recommend that you evaluate the ENISA training material (see http://www.enisa.europa.eu/activities/cert/training), where you find tens of trainings and exercises covering technical, operational, legal and co-operation aspects. Materials and documentation are all available online, including technical resources.
- CERT Division. CERT Division (Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA, USA, home of CERT Coordination Center or CERT/CC) offers courses in the areas of creating and managing a CSIRT, incident handling, network security, risk assessment, resilience management, and insider threat. These courses have attendance fees and are generally held in the USA, but have been taught in various countries. They can be held on site, upon request. CERT also licenses its courses and provides a train-the-trainer program. For more information see https://www.cert.org/training/. Through the STEPfwd program, distance and online education is possible. For more information see https://stepfwd.cert.org/.
- SANS. The SANS Institute is a commercial organisation offering a very wide range of security related trainings, both live and online, including a few directly CSIRT related trainings (look under "Security" and "Management"). Some courses are held all over the world, others mostly in the USA. Check it out online at https://www.sans.org.

[6] TRANSITS also offers some more advanced training modules, e.g. about forensics, netflow and human communication – on demand.

4 TOOLS

Without proper tools your team members cannot do their work – they would get lost in trivial details. Especially when the incident load (the number of reported incidents per day) goes up, tools become mission critical. Particularly automated tools are one of the most important aspects for research and investments of today's CSIRTs. In this chapter we survey some of the most essential tools. You will also find some tools mentioned as part of the descriptions in chapter 5.

4.1 IT Resources List

As the CSIRT for your constituency you should know what kind of information your constituency expects from you. This means you need to know what kind of hardware and software they use – more generally you need to know about their IT assets You should pay particular attention to knowing what the vital assets are, especially in the sense of the primary/business processes. If you service a single organisation you will also want to know the network architecture and topology – these too are IT assets.

Bigger, especially commercial organisations may well use some form of standardized IT asset management, following the guidance of such standards as ISO-27002 ("Asset management"), or ITIL ("Configuration Management Database"). In that case the CSIRT should be able to use that information to suit the needs of the constituency.

However such centralized and accurate asset management is generally rare. Especially in a heterogeneous, not tightly managed constituency, we advise to directly ask your constituents which platforms and software they use, and what their information needs are. A good way of doing this is by asking them to fill out a detailed questionnaire – followed by a site visit following that to discuss any unclarities in the information provided. This "snapshot" of their IT assets should be given some form of continuity, by means of a sanity check once every year, and a repeat site visit every 3 years. Of course such a "snapshot" scheme has an additional purpose, as it will become a very useful part of the outreach of your team towards your constituency (see 5.5).

4.2 Consolidated E-Mail System & Incident Tracking System

Your CSIRT needs to have a consolidated system that handles incoming and outgoing e-mail and tracks incidents. This means that each incident will be numbered and all relevant information, including e-mail, will be ordered accordingly. Some form of workflow management is also needed, so that at least incidents can be opened, tracked and closed. An incident classification scheme (see 2.3) should be used in the system to categorize all incidents.

There are many types of "incident management" software that can perform tasks like this, but very few are tailored towards CSIRTs. Some popular ones among CSIRTs are:

- RTIR, which was developed for CSIRTs: https://bestpractical.com/rtir/
- OTRS, open source incident management system: https://www.otrs.com
- AIRT, freely available tracking tool with decent automation features: http://airt.leune.com

There is an on-going development that commercial software vendors are entering this scene. Two examples of promising software in this area that seem mostly targeted at CSIRTs internal to bigger organisations[7]:

- https://www.resilientsystems.com/product/security
- http://cybersponse.com

As part of the e-mail system you need to make sure that standard e-mail addresses for your organization's domain name are covered either by your team, or by IT colleagues in the organization who know about your team and know that they need to forward any security incident related e-mail to you. The standard addresses to cover can be found in the Common Mailbox Names rfc (see http://www.rfc-editor.org/rfc/rfc2142.txt). As a pragmatic way to handle emails, we suggest to cover:

security@ ; cert@ : by your CSIRT
abuse@ : by either your CSIRT or your organisation's abuse handling team
postmaster@ ; hostmaster@ ; webmaster@ ; www@ : by appropriate IT staff

Finally, in order to exchange confidential e-mail the de facto standard used worldwide between CSIRTs is pgp/gnupg. It's simply a **must** for any CSIRT working together with other teams to set up a system where the team has a pgp team-key that others can use to send information encrypted to your team. And additionally, individual pgp keys for at least those team members representing the team to the world, but preferably for all team members: this is to enable the team members to sign confidential e-mail so that the recipients are sure it comes from them. For the open source GnuPG see https://www.gnupg.org ; for the commercial PGP see http://www.pgp.com .

One of the most reliable guides to gnupg – many of which also applies to pgp – is this FAQ: https://www.gnupg.org/faq/gnupg-faq.html . As it says there, it is important for good security to choose the right encryption key type and length: the safest available combination at the moment is RSA with a keylength of 4096 bits[8]. The most frequently used toolsets to get started with gnupg are:
for Microsoft Windows (including Outlook): http://www.gpg4win.org ;
for Mac OS X: https://gpgtools.org ;
for Linux: https://www.gnupg.org/faq/gnupg-faq.html#get_gnupg .

5 PROCESSES

In this chapter you will find a collection of best practices regarding processes that we recommend you give consideration, document, implement and act upon. Process in this context can be read as "policy" or "plan" , but we do not adhere to a strict process definition as some sort of workflow diagram. In fact we recommend that you document the following processes/policies/plans in concise and simple ways, and make them readily available for use. Many CSIRTs choose to make these available through e.g. internal wiki pages, so that every team member can easily access them and they can be linked from other pages, workflow descriptions etcetera. That way they are integrated in the daily operations, instead of becoming just a "reference handbook", which usually are referenced very little. Keep it simple: integrate your processes in your operations.

[7] Note: few CSIRT references so far, so no recommendation here yet.
[8] A minimum RSA keylength of 2048 bits is required for safety today.

5.1 Threat & Incident Detection Process

You need to determine your sources for the detection of threats and incidents, and you need to document these in a pragmatic process, e.g. on your team's wiki.

Your sources include your constituency and other CSIRTs who can all report to you, but you should also gather your own intelligence from various sources that are related to the sector of your your specific CSIRT or your specific constituency.

A useful reference in this regard is the ENISA Guide for Alerts, Warnings and Announcements: https://www.enisa.europa.eu/activities/cert/support/awa .

Some excellent tools to support this process:

i. TARANIS: a tool by NCSC-NL which makes it much easier to manage a multitude of information sources and derive alerts/warnings in a structured way. See https://www.ncsc.nl/english/services/incident-response/monitoring/taranis.html .
ii. AbuseHelper: a tool initiated by NSCS-FI and CERT-EE that is mainly intended for the automated handling of information sources. See http://www.abusehelper.be . There is also a commercial version available at https://www.clarifiednetworks.com/AbuseSA .
iii. IntelMQ: a tool similar to AbuseHelper but newly developed by an initiative of CERT.at and RCTS CERT. See https://github.com/certtools/intelmq .
iv. MISP: Malware Information Sharing Platform. See http://www.misp-project.org.

Regarding automated data sharing you should be cautious of the great multitude of existing standards and formats, many of which are not really in use by CSIRTs. We strongly advise you to join existing working groups in this field for your region, or inside FIRST. Even when you are using a standard, automated data sharing only works when **all parties** involved agree on **all details** of the standard. A very useful reference to read in this area is: http://www.enisa.europa.eu/activities/cert/support/actionable-information

5.2 Incident Resolution Process

The next step is to document the process of resolving incidents. This includes who your trusted communication partners are (especially within your constituency and which other CSIRTs), what tools you use to track and analyse incidents, how to use them, etcetera.

A useful reference is ENISA's Good Practice Guide for Incident Management: https://www.enisa.europa.eu/activities/cert/support/incident-management.

5.3 Emergency Accessibility Process

You need to consider how accessible your CSIRT should be in case of emergencies, outside your normal office hours, and to whom you will publish this emergency accessibility information: to your constituency? to trusted CSIRTs? others? Document this in a process, and publish it at the appropriate places.

Some suggested places to consider to publish such information, but it really depends on the choices that you make in this regard:

- On your team's webpage for your constituency or organisation.
- On your team's public webpage. We repeat the advice to have a team webpage or "slash security page" for your organisation: see 2.2.
- In your team's rfc-2350: again see 2.2.

- If you are a FIRST member: in the information only available to FIRST members? Or in the publicly available information?
- If you are a member of a transnational or sectoral CSIRT cooperation forum, the same consideration applies;most of these forums will have publicly available information, plus information only for members.
- Spread the word to other CSIRTs that you have a special relationship with e.g. your national CSIRT, or the CSIRT of the Internet Service Provider for your organisation.

5.4 Information Handling Process

You need to consider carefully and then document how you handle, share and disclose information.

Moreover, your constituents and other CSIRTs expect that your team is capable of handling information in a **secure** way, and will do so by default. This means that you need to think about such things as:

- Secure e-mail (you must support pgp/gnupg: see 4.2)
- Secure storage
- Secure back-ups (also off-site)
- Physical security
- Secure destruction of information and media (such as hard disks)

We advise you to document your information handling process in a pragmatic way, e.g. on your team's wiki. Your process should include:

i. An internal document classification. A simple, useful classification containing 3 classes: public, internal and confidential. Remember, once you classify, you need to remember actions for **each** of the classifications: so the fewer, the simpler, the better. Some of you will be in an organisation that already has such a classification (especially big companies, government, military): in which case you must support that, sometimes this may be required by law.
ii. We strongly advise that you use the de facto standard called ISTLP: Information Sharing Traffic Light Protocol, towards other CSIRTs and towards your constituency. ISTLP is used by an increasing number of CSIRTs worldwide; it's simple and it's effective. You should at **least** acknowledge its existence. See e.g. https://www.terena.org/activities/tf-csirt/publications/ISTLP-v1.1.pdf .

5.5 Constituency Outreach Process

We recommend that you consider how to structurally reach out to your constituency, so not only incident driven. Document this in your constituency outreach process. This process could contain elements for your constituents such as:

- Newsletters
- Seminars or workshops
- Going out and meeting your constituents one-on-one (see also 4.1)
- Trainings
- Your team's webpage
- E-mail distribution list(s)
- Use of social media

5.6 Media Relations Process

We recommend that you consider how to relate to the public media, and to document that. This can be as simple as "the CSIRT does not deal with the public media, all such cases are referred to the organisation's press office". Or it can describe who deals with the media, and how. If one or more of your team members are allowed to talk with the press they should get specific training for that. It takes skill and experience to do this in a constructive way, without disclosing more than intended.

5.7 AUP & Security Policy

An AUP or Acceptable Use Policy describes which use of network and computers by your team members is considered as acceptable: e.g. only for professional use or also for private use. The Security Policy is the framework for maintaining internal information security.

Both are important policies, and every CSIRT needs to think about these matters, but in many cases these policies are provided on the level of the parent organisation. If that is not the case, your CSIRT needs to document them for your own sake.

We mention these policies specifically, because you need to consider the fact that the CSIRT often has to be an "exception to the rules". For instance: in general you want your employees not to click on suspicious links – but your CSIRT team members may need to do so as part of their analysis work, and then if they do, they should have test systems for that, not their regular computer. Your organisation's firewall may have various useful filters to protect your business processes; however, the CSIRT needs to be able to have unfiltered access to the Internet for testing purposes. This can be achieved by a separate connection, tying in to a test network. These are all arguments to either document your own AUP and Security Policy, or to use that of your organisation, but to document the "exceptions to the rules" for your CSIRT to be able to do its work properly.

6 CONCLUSION

This CSIRT Maturity Kit offers a reference for CSIRTs. With this kit, teams can gain insight in important areas where they can improve their current level of maturity – and then hopefully use those insights to actually implement these improvements. As teams mature and evolve, they will increase their capacity to handle the ever-changing cyber threat landscape. As capacity increases, so does the ability to assist other teams. Improving the maturity of one team thus benefits other teams in your network. Cyber security is a shared responsibility and requires a joint effort. Increasing your maturity level is therefore vitally important to the entire CSIRT community.

In addition to its reference function, this document is also intended as a basis for further international discussion on this topic and the exchange of best practices. An open, honest discussion is essential to building trusted relationships. This document is therefore not the final version on this subject, but rather an invitation for suggestions. Joining in this discussion and sharing your experience/expertise will not only improve the content of future versions of this document, but will also strengthen the community and increase our joint capacity.