Study on CSIRT Maturity – Evaluation Process

VERSION 1.0

26 MAY 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Editors

ENISA

Contact

For contacting the authors please use cert-relations@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank CISRTs Network experts who contributed to this study for their valuable insight during the project. Namely we would like to thank Mr. Olivier Caleff from CERT-FR and Mr. Martijn De Hammer from NCSC.NL for their valuable insight during the review phase of the project.

ISBN 978-92-9204-223-3, DOI 10.2824/35988

Table of Contents

Executive Summary

The primary target audience for this report is the EU CSIRTs network teams, and their leadership. However it needs to be stressed here that this report, and especially the maturity self-assessment that it contains, will be of use to all types of CSIRTs all over the world.[1]

The EU Network and Information Security Directive[2] (NIS Directive) creates a CSIRTs network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process. The Directive gives high-level requirements that designated CSIRTs must observe, and tasks that they must perform.

In order to provide input to the designated CSIRTs on this topic, ENISA performed a continuation of the 2016 study on CSIRT maturity, focused on the national teams expected to join the CSIRTs network. To recapitulate, the 2016 study had the following main results:

1. A sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NIS Directive requirements.

2. The three-tier approach towards maturity that ENISA adopted in the 2013 report "CERT community - Recognition mechanisms and schemes" can be used to define a scale of three steps when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and certifiable.

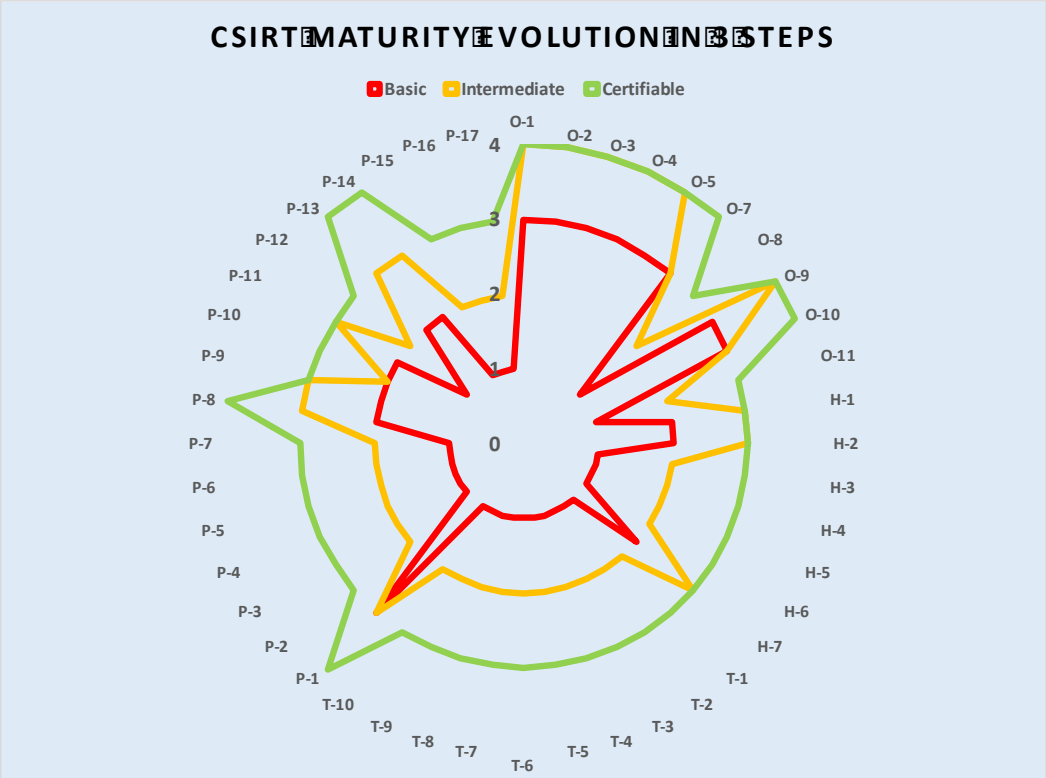
3. A proposed specific definition of those three steps for the benefit of the CSIRTs network, coupled with the suggestion to define a validation process based on self-assessments and peer-assessments.

By adopting the approach proposed in the 2016 study, the CSIRTs network would have immediate access to a clearly laid out CSIRT maturity improvement process, that is not only implementable and sustainable, but also based on a proven best practice: the SIM3 model is in use in the European TF-CSIRT Trusted Introducer community since 2009, for self-assessments but also for over 20 certifications so far, including 5 members of the CSIRTs network.[3] The Global Forum on Cyber Expertise (GFCE[4]) has adopted

[1] Only in the definitions of the three maturity steps, there are elements that are strongly based on EU NISD demands – however these three steps can easily be adapted to the demands in other CSIRT cooperations, regions and/or sectors.
[2] http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement/
[3] The 5th certification is being processed at the moment of writing this.
[4] https://www.thegfce.com

SIM3 as their CSIRT maturity framework in 2015.[5] In Japan, the Nippon CSIRT Association (NCA[6]), with well over 200 member teams, is basing their maturity improvement scheme on SIM3.

A growth path was suggested that reaches the basic step within one year, intermediate two years later and certifiable another two years later: a total of five years' maximum which is in line with the CSIRTs network work roadmap. Achieving the basic step would already allow a minimum of successful co-operation between teams on incident handling, the higher steps are needed to allow the members of the CSIRTs network to interact on all steps, including pro-actively, thus truly giving meaning to the word CSIRTs network.



The continuation work reported on here focused on two important aspects of the afore mentioned CSIRT maturity improvement process:

1. Self-assessment survey. A survey with questions and answers for all the SIM3 parameters is delivered here, which makes it considerably easier for any team to self-assess their maturity in the terms of SIM3. The survey is complete with a mapping to the proposed CSIRTs network maturity scale (with the steps basic, intermediate and certifiable), so that members of the CSIRTs network who use the survey can self-assess their maturity on that scale.

2. Peer review methodology. A methodology for how to do peer reviews inside the CSIRTs network is delivered here, complementary to the self-assessment approach and intended as a form of

[5] See the GFCE's "CSIRT Maturity Kit": https://check.ncsc.nl/static/CSIRT_MK_guide.pdf
[6] http://www.nca.gr.jp/en/

intra-community mutual support aimed at further enhancing all teams' maturity. The proposed peer review approach is a flexible one, that is expected to suit the needs of all teams involved.

With all these building blocks in place, the next recommended step is discussion inside the CSIRTs network, followed by a small scale pilot application, any necessary revisions, and then roll-out. During the whole process it is recommended to stay in close touch with the (not-for-profit) Open CSIRT Foundation [1], who have assumed the SIM3 stewardship role in October 2016, to make sure that the SIM3 related developments are handled synergistically.

1. Introduction

The EU Network and Information Security Directive (NIS Directive) aims to create a CSIRTs network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". [2] The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in the Directive's point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process. The Directive gives high-level requirements that designated CSIRTs must observe, and tasks that they must perform.

ENISA's 2016 study on CSIRT maturity, focused on the national teams expected to join the CSIRTs network, concluded that a sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters, and it proposed to use the existing SIM3 model for that. The existing ENISA three-tier maturity approach was added to define a scale of three steps when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and certifiable. It was proposed to validate these inside the CSIRTs network by means of a process based on self-assessments and peer-assessments.

In order to further explain this validation process, ENISA has contracted a research to establish a readily implementable and useable self-assessment survey and peer review methodology. The results of this study are presented here.

2. Methodology

The work carried out in this project focused on how to measure the maturity of CSIRTs, especially those in the CSIRTs network, by means of self-assessment (chapter 3) and peer review (chapter 4) based on the SIM3 maturity model (see 2.1). This work is a practical follow-up of the recommendations made in the ENISA report: *Challenges for National CSIRTs in Europe in 2016 : Study on CSIRT Maturity* (2016).

2.1 Input sources

Input was considered from the following areas:

1. The ENISA report *Challenges for National CSIRTs in Europe in 2016 : Study on CSIRT Maturity* (2016) [3]
2. The SIM3 model for CSIRT self-assessment and certification (generic evaluation scheme for any type of CSIRT) [4]
3. The NIS Directive – tasks and requirements of the dedicated (national) CSIRT (obligations for national (dedicated) CSIRT in the European Union [5]

2.2 Input evaluation

Members of two CSIRTs network teams provided advice and input, as did the Open CSIRT Foundation.

3. Self-assessment Survey

This chapter details a survey that teams can use to self-assess their team's maturity in terms of the SIM3 model. The outcomes of such self-assessments will in principle be less objective than can be expected from e.g. the TI Certification, which is also based on SIM3. However, for the purpose of the CSIRTs network and this report, we see this survey as a fair and useful approximation, especially when combined with peer review (see chapter 4).

The survey is self-explaining. Simply follow the questions for all 44 SIM3 parameters, and select the answer that fits your situation best. This will result in a self-assessed level for each of the 44 parameters. These levels can be one of the following (taken from the SIM3, with NOTEs added):

Level	Explanation
0	Not available / undefined / unaware.
1	Implicit (known/considered but not written down, "between the ears").
2	Explicit, internal (written down but not formalised in any way). NOTE: any written document (including wiki pages) that has not been formally approved by the CSIRT management falls in this category.
3	Explicit, formalised on authority of the CSIRT management ("rubberstamped" or published). NOTE: any written document (including wiki pages) that has been formally approved by the CSIRT management falls in this category. Bear in mind that if a document has been formally approved at an organisational level that is hierarchically *above* but in the *same branch* of the (host) organisation's organigram, that document is automatically valid for the CSIRT and their management too – still, if it is directly relevant, it is advisable for the CSIRT management to endorse this document anyway, and e.g. place it on the team wiki. (As to such a team wiki, if it exists, we advise that if that holds level 3 documents, to use version and date control, to ensure that a document that has once been approved by the CSIRT management, does not automatically keep that status forever. Otherwise the risk of having outdated documents is significant.)
4	As 3, but regularly and explicitly assessed on authority of governance levels above the CSIRT management. NOTE: in the answers below we talk about "periodic review". Often that period does is one year. It can however also be twice per year for instance, or once per

	2 years for instance. What matters is that it is regular, and planned and will actually take place. What is also important is that parameters are "explicitly" assessed or reviewed: and this needs to be laid down in writing explicitly. So a vague statement like "the team will be reviewed every year" does not lead to level 4 for all SIM3 parameters – the parameters in question, or their content, must be explicitly mentioned, and explicitly reviewed. The review must be on the initiative of the higher levels of management: not the CSIRT management. This also means that sending a periodic report to the higher management does not allow a level 4 status – that is still level 3. There is one special case: if a parameter is *explicitly* mentioned (by content, not necessarily by name) in national law, then this allows a level 4 status, because we assume that in all EU countries, national law is sufficiently maintained and guarded by all 3 powers of the Trias Politica [7]– we do repeat here that the parameter's content must be made *explicit* in the law, no vague abstractions.

Finally, we added for each parameter the proposed minimum steps for "basic", "intermediate" and "certifiable" maturity as has been proposed for the CSIRTs network. This way, using this survey for self-assessment, a team can quickly see where they are maturity wise. Of course, "basic" maturity is reached when all parameters score "basic" or better. "Intermediate" maturity is reached when all parameters score "intermediate" or better. And the same for "certifiable".

3.1 O – Organisation parameters

3.1.1 O-1: Mandate

Question

Does your CSIRT have a mandate? The mandate defines the assignment of your team. Ideally, the mandate is set at the highest management or political level (in the latter case it can even be anchored in legislation).

Answers

- We never really discussed this and we don't formally know our mandate or assignment. We just do our work. ➔ level 0
- We have a pretty good idea that we are doing is what we were assigned to do, but it was never written down. ➔ level 1
- We don't have a formal written mandate, therefore we wrote something for our own purposes. Our team management has not formally approved this. ➔ level 2
- We have a written mandate approved by our team management. ➔ level 3
- We have a written mandate from higher management that our team management regards as authoritative. In the periodic review of our team it is checked if and how we fulfil our mandate. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

[7] https://en.wikipedia.org/wiki/Separation_of_powers

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.2 O-2: Constituency

Question

Does your CSIRT have a clear constituency, that is, the target group for who you do the CSIRT work, your "client base"? The constituency can be internal to your organisation, or it can be external (or both).

Answers

- We never really discussed this. ➔ level 0
- We know our constituency, but it was never written down. ➔ level 1
- We don't have a formal written constituency definition, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written constituency definition approved by our team management. ➔ level 3
- We have a written constituency definition approved by our team management. In the periodic review of our team it is checked if and in how far we serve this constituency, and whether the definition needs to be adapted. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.3 O-3: Authority

Question

What is your CSIRT **allowed** to do towards your constituency in order to accomplish your role and satisfy your mandate? Your team's authority could range from advisory only, towards enforcement and/or escalation options.

Answers

- We never really discussed this. ➔ level 0
- We know our authority, but it was never written down. ➔ level 1
- We don't have a formal written authority definition, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written authority definition approved by our team management. ➔ level 3
- We have a written authority definition approved by our team management. In the periodic review of our team it is checked if and how we align with this authority, and if it is sufficient to meet our mandate. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.4 O-4: Responsibility

Question

What is your CSIRT **expected** to do towards your constituency in order to accomplish your role and satisfy your mandate?

Answers

- We never really discussed this. ➔ level 0
- We know our responsibility, but it was never written down. ➔ level 1
- We don't have a formal written responsibility definition, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written responsibility definition approved by our team management. ➔ level 3
- We have a written responsibility definition approved by our team management. In the periodic review of our team it is checked if and how we meet this responsibility. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.5 O-5: Service Description

Question

What are the services that your CSIRT offers to their constituency? This could include different services such as incident response, vulnerability handling, malware analysis and others - plus related practical aspects like contact information and service windows. An important aspect to consider is whether a version of the service description has been made available to (at least) the constituency – to publish rfc-2350 is a recommended way of doing this.

Answers

- We never really discussed this. We just do our work. ➔ level 0
- We know what services we offer, but it was never written down. ➔ level 1
- We don't have a formal written service description, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written service description approved by our team management, and it has been made available to our constituency. ➔ level 3
- We have a written service description approved by our team management, and it has been made available to our constituency. In the periodic review of our team it is checked if and how we provide these services. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.6 O-6: not available

Parameter O-6 is not in use anymore. For reasons of backwards compatibility, it has been intentionally left blank.

3.1.7 O-7: Service Level Description

Question

Have service levels been defined for the services that your CSIRT offers? This can range from something as simple as the requirement to send a first (human) reaction to incident reports within a set amount of time, to more extensive "SLA" type requirements.

Answers

- We never really discussed this. ➔ level 0
- We have a basic understanding of the level of service expected of us, but it was never written down. ➔ level 1
- We don't have a formal written service level description, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written service level description approved by our team management. ➔ level 3
- We have a written service level description approved by our team management. In the periodic review of our team it is checked if and how we meet our service level(s). ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 3 or better
- Certifiable: level 4

3.1.8 O-8: Incident Classification

Question

Does your CSIRT use an incident classification scheme when recording incidents? Incident classifications usually contain "types" of incidents or incident categories. However, it is highly recommended that they also include the aspects "severity/impact" and "priority" – as this will allow a logical way of dealing with bigger number of incidents at the same time, and also indicate when escalations may be due (see e.g. P-1,2,3).

Answers

- We don't classify incidents, we just deal with them. ➔ level 0
- We appreciate that there are different types of incidents, but we don't make this explicit. If an incident needs special attention, we just deal with that accordingly. ➔ level 1
- We don't have a formal written incident classification, therefore we wrote one for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written incident classification approved by our team management. ➔ level 3
- We have a written incident classification approved by our team management. In the periodic review of our team attention is given to the different types of incidents and how we handled those. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.1.9 O-9: Participation in Existing CSIRT Frameworks

Question

Does your CSIRT participate in a well-established CSIRT co-operation, either directly or through an "upstream" CSIRT of which your team is a customer/client? This kind of participation is necessary to be an effective member of the national/sectoral/regional/worldwide CSIRT collaboration.

Answers

- We never really discussed this. ➔ level 0
- We know in what CSIRT co-operation(s) we participate, but it was never written down. ➔ level 1
- We don't have a formal written statement on the CSIRT co-operations we participate in, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written statement on the CSIRT co-operation(s) we participate in, approved by our team management and budget supported. ➔ level 3
- We have a formal written statement on the CSIRT co-operation(s) we participate in, approved by our team management and budget supported. In the periodic review of our team it is checked if and how actively we participate in these co-operations, and what the benefits are. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 4
- Certifiable: level 4

3.1.10 O-10: Organisational Framework

Question

Does your CSIRT have a coherent framework document serving as the controlling document for the team, also known as "team charter" or "organisational framework"? This charter should bundle descriptions for O-1 to O-9 and possibly some more SIM3 parameters. In many cases, teams seek the approval of the higher management of their organisation for their charter - recommended, but not obligatory. Rfc-2350 is sometimes proposed as a team charter, but though rfc-2350 does cover some of the "O" parameters, it does not cover all of them, and more importantly is not meant to be a controlling document, but rather a public service description for a CSIRT.

Answers

- We never really discussed this. ➔ level 0
- We do have a coherent view on our organisational set-up, but it was never written down. ➔ level 1
- We don't have a formal written organisational framework, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written organisational framework approved by our team management. ➔ level 3

- We have a written organisational framework approved by our team management. In the periodic review of our team, it is tested if the framework is up-to-date and effective. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 3 or better
- Intermediate: level 3 or better
- Certifiable: level 4 or better

3.1.11 O-11: Security Policy

Question

Does your CSIRT or its host organisation have a security policy or framework within which your team operates? The policy for your team can be an explicit or implicit part of a policy for the wider organisation - or your CSIRT may have a separate security policy. As a CSIRT usually has specific IT/security requirements (e.g. wanting to receive unfiltered e-mail, needing to have some way of running tests without being blocked by a firewall, specific encryption demands, etc.), a separate policy is worth considering.

Answers
- We never really discussed this. ➔ level 0
- We know the kind of security limitations that apply, but those were never written down. ➔ level 1
- We don't have a formal written security policy that applies to us, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written security policy that applies to us, approved by our team management. ➔ level 3
- We have a written security policy that applies to us, approved by our team management. In the periodic review of our team it is checked if we meet this policy and if it works for us. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.2 H – Human parameters

3.2.1 H-1: Code of Conduct/Practice/Ethics

Question

Does your CSIRT have a set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work – confidentiality and trustworthiness being among the key qualities. The Trusted Introducer CSIRT Code of Practice serves as an example, and can be used for this purpose. A code of conduct for the team's host organization may exist, but is rarely sufficient as it does not touch on the specific CSIRT aspects.
Note: behaviour outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.

Answers

- We never really discussed this. ➔ level 0
- We know what kind of work ethics are expected of us, but they were never written down. ➔ level 1
- We don't have a formal written code of conduct, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written code of conduct approved by our team management. ➔ level 3
- We have a written code of conduct approved by our team management. In the periodic review of our team it is checked if and how this code has been used and if it serves its purpose. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 3 or better

3.2.2 H-2: Personal Resilience

Question

Is your CSIRT's staffing sufficiently ensured, also when one or more members go ill, are on holiday, quit their job, etcetera? Three (part-time) team members are seen as an absolute minimum to ensure that at any point in time at least someone can pick up the phone, or read e-mail and do something. Depending on the services offered and the service level agreements, a significantly bigger number (permanent and/or ad hoc) may be required to ensure availability even in times of short-term challenges or crises.

Answers
- This is outside our scope. ➔ level 0
- We do have sufficient people on the job to be resilient, but this was never put down in writing. ➔ level 1
- We don't have a formal statement on the number of available CSIRT staff, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal statement on the number of available CSIRT staff approved by our team management. ➔ level 3
- We have a formal statement on the number of available CSIRT staff approved by our team management. In the periodic review of our team it is checked how the staffing situation was, and if there was sufficient resilience. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 3 or better

3.2.3 H-3: Skillset Description

Question

Does your CSIRT have a description of the skills needed on the CSIRT position(s) that you have inside your team? These can be positions like "(senior) incident handler", "cyber security researcher", "general manager", and others. Skills should not only be of a technical/knowledge nature, as also soft skills are essential to the CSIRT work, such as communication and presentation skills, team play, flexibility.

Answers

- We never really discussed this. Our staff are experienced. ➔ level 0
- We know what kind of skills we need to have, but they were never written down. ➔ level 1
- We don't have a formal written skillset description, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a written skillset description approved by our team management. ➔ level 3
- We have a written skillset description approved by our team management. In the periodic review of our team it is checked if this skillset is sufficient to tackle current threats and incidents. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.2.4 H-4: Internal Training

Question

Does your CSIRT (or host organization) offer any form of internal training in order to train new team members and to improve the skills of existing ones, on topics relevant to the CSIRT work? This can be on-the-job-training as well as classroom-type or other types of traditional training.

Answers

- We don't offer this kind of training. ➔ level 0
- We have ideas about internal training and/or we train team members informally, but we never wrote down anything about training demands, topics or materials. ➔ level 1
- We don't have a formal internal training programme, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have an internal training programme approved by our team management. ➔ level 3
- We have an internal training programme approved by our team management. In the periodic review of our team it is checked if this internal training programme has been put into action sufficiently to meet the training needs of the team. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.2.5 H-5: (External) Technical Training

Question

Does your CSIRT allow staff to get relevant job-technical training? This is usually done externally – like TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.) – but in some bigger organisations such trainings are also (partially) available internally.

Answers

- We have no options, time or money for this kind of training. ➔ level 0
- We send people to such trainings when it is necessary, but we have no written policy on this. ➔ level 1
- We don't have a formal technical training programme, therefore we wrote something for our own purposes which helps in sending our staff to such trainings. Our management has not formally approved this programme. ➔ level 2
- We have a technical training programme approved by our team management, which allows us to send our staff to such trainings. ➔ level 3
- We have a technical training programme approved by our team management, which allows us to send our staff to such trainings. In the periodic review of our team it is checked if this technical training programme has been used sufficiently to meet the training needs of the team. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.2.6 H-6: (External) Communication Training

Question

Does your CSIRT allow staff to get relevant communication training? This is usually done by external trainers but in some bigger organisations such trainings are also available internally. Note that this parameter is not just about talking with the press: in every aspect of the CSIRT work, human communication is of the utmost importance, whether this is in writing e-mails or advisories, or talking to people on the phone or in meetings. It might include crisis communication, which for some CSIRTs (e.g. national and government teams) is an important topic.

Answers
- We have no options, time or money for this kind of training. ➔ level 0
- We send people to such trainings when it is necessary, but we have no written policy on this. ➔ level 1
- We don't have a formal communication training programme, therefore we wrote something for our own purposes which helps in sending our staff to such trainings. Our management has not formally approved this programme. ➔ level 2
- We have a communication training programme approved by our team management, which allows us to send our staff to such trainings. ➔ level 3
- We have a communication training programme approved by our team management, which allows us to send our staff to such trainings. In the periodic review of our team it is checked if this communication training programme has been used sufficiently to meet the training needs of the team. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.2.7 H-7: External Networking

Question

Are your CSIRT members sent to meetings with other CSIRTs and other relevant cyber security professionals? This does not only improve the level and effectiveness of your own team, but also contributes to the worldwide CSIRT collaboration, which again is essential for the success of all, including your CSIRT.

Answers

- We have no options, time or money for this kind of activity. ➔ level 0
- We go to such meetings when we can, but nothing has been written down about it. ➔ level 1
- We don't have a formal written statement on our external networking, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written statement on our external networking, approved by our team management. ➔ level 3
- We have a formal written statement on our external networking, approved by our team management. In the periodic review of our team it is checked if and how actively we pursue our external networking, and what the benefits are. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 3 or better

3.3 T – Tools parameters

3.3.1 T-1: IT Resources List

Question

Does your CSIRT have access to a list or database that describes the hardware, software, etc. commonly used in the **constituency**, or at least in vital parts of the constituency, so that the CSIRT can provide targeted advice? This question is about "asset management" (ISO terminology) or the "Configuration Management Database" (CMDB: ITIL terminology). The CSIRT will normally not maintain a CMDB, but at least they need to have access to it if it exists. In the absence of an advanced solution, the CSIRT may consider maintaining a limited version of such a list themselves, with the help of their security contacts in the constituency.

Note: in the case of e.g. national teams, or university teams, it can be argued that the constituency uses all possible types of IT resources, and that it is therefore not feasible to maintain such a list. In such cases it is acceptable in the case of T-1 that the CSIRT focuses on "vital parts of the constituency", like a country's critical infrastructure, or a university's business and core IT systems – and that at least for those vital parts, the CSIRT should know what kind of IT resources are being used.

Answers

- We don't really know. ➔ level 0
- We have a good idea of the most important IT resources, but there is no list for this. ➔ level 1

- We don't have a formal IT resources list, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have access to a formal IT resources list, and this has been approved by our team management. ➔ level 3
- We have access to a formal IT resources list, and this has been approved by our team management. In the periodic review of our team it is checked if this list is useful and sufficiently accurate for the goals of our team. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.2 T-2: Information Sources List

Question

Does your CSIRT maintain a list of sources (info feeds, websites, newspapers, tweets, etc.) where they get their vulnerability/trend/scanning information from? When such a list exists, it should have some form of importance rating of the sources – e.g. splitting them in primary, secondary and tertiary sources.

Answers
- We don't have any such list. We don't systematically check sources but instead react to incident reports. ➔ level 0
- We know our most important sources and check them out, but there is no list for this. ➔ level 1
- We don't have a formal list of information sources, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal list of information sources approved by our team management. ➔ level 3
- We have a formal list of information sources approved by our team management. In the periodic review of our team it is checked if this list is useful and sufficient for the goals of our team. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.3 T-3: Consolidated E-mail System

Question

Does your CSIRT keep all CSIRT e-mail in one repository open to all team members?

Answers
- The CSIRT e-mail goes to the laptops/computers of the team members. There is no need to keep it in one place. ➔ level 0
- We keep CSIRT e-mail in one repository, but this system is not under our control and we don't know much about it. ➔ level 1
- We keep CSIRT e-mail in one repository. Our management has not formally approved this. ➔ level 2

- We keep CSIRT e-mail in one repository and this was approved by our team management. ➔ level 3
- We keep CSIRT e-mail in one repository and this was approved by our team management. In the periodic review of our team it is checked if this repository meets our requirements. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.4 T-4: Incident Tracking System

Question

Does your CSIRT use a trouble ticket / workflow management system, open to all team members, to register incidents and track their workflow? Typical examples of such systems are RT(IR), OTRS, or generic trouble ticket systems – smaller teams sometimes use simpler solutions like a shared spreadsheet.

Answers
- We solve incidents, we don't have a registration tool for them. ➔ level 0
- We have a way of registering and tracking incidents, but have not documented it. ➔ level 1
- We have an incident tracking system. Our management has not formally approved this. ➔ level 2
- We have an incident tracking system and this was approved by our team management. ➔ level 3
- We have an incident tracking system and this was approved by our team management. In the periodic review of our team it is checked if this tracking systems meets our requirements. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.5 T-5: Resilient Phone

Question

Do the uptime and time-to-fix service levels of the telephone system available to your CSIRT meet or exceed your team's service levels? That is: if the phone system goes down, can you expect it to be fixed quick enough for you to still be able to meet your service levels? Bear in mind in this regard, that telephony is more and more IP based. Mobile phones are usually the fallback mechanism for when a team's standard phone system is out of order – and at least it should be possible to call out under those circumstances. Satellite phones are another option, and some teams may have access to special, extra secure, telecommunication infrastructures.

Answers
- We don't really know anything about the service levels of our phone system, and we haven't arranged any fallback scheme (e.g. using mobile phones). ➔ level 0
- When the phone system goes down we adopt a fallback scheme (e.g. using mobile phones), but we have not documented this. ➔ level 1

- When the phone system goes down we adopt a fallback scheme (e.g. using mobile phones) and we documented this. Our management has not formally approved this. ➔ level 2
- When the phone system goes down we adopt a fallback scheme (e.g. using mobile phones), we documented this and this was approved by our team management. ➔ level 3
- When the phone system goes down we adopt a fallback scheme (e.g. using mobile phones), we documented this and this was approved by our team management. In the periodic review of our team it is checked if this fallback scheme meets our requirements and is sufficiently known. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.6 T-6: Resilient E-mail

Question

Do the uptime and time-to-fix service levels of the e-mail system available to your CSIRT meet or exceed your team's service levels, a situation described in the answers below as "good enough for our purposes"? That is: if the e-mail system goes down, can you expect it to be fixed quick enough for you to still be able to meet your service levels?

Answers

- We don't really know anything about the service levels of our e-mail system. ➔ level 0
- The service level of our e-mail system is good enough for our purposes, but we have no documentation for this. ➔ level 1
- The service level of our e-mail system is good enough for our purposes, and we have informal documentation for this. Our management has not formally approved this. ➔ level 2
- The service level of our e-mail system is good enough for our purposes, and we have documentation for this that was approved by our team management. ➔ level 3
- The service level of our e-mail system is good enough for our purposes, and we have documentation for this that was approved by our team management. In the periodic review of our team it is checked if this e-mail resiliency is sufficient. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.7 T-7: Resilient Internet Access

Question

Do the uptime and time-to-fix service levels of the Internet access available to your CSIRT meet or exceed your team's service levels? That is: if the Internet access goes down, can you expect it to be fixed quick enough for you to still be able to meet your service levels?

Answers

- We don't really know anything about the service levels of our Internet access. ➔ level 0
- The service level of our Internet access is good enough for our purposes, but we have no documentation for this. ➔ level 1
- The service level of our Internet access is good enough for our purposes, and we have informal documentation for this. Our management has not formally approved this. ➔ level 2
- The service level of our Internet access is good enough for our purposes, and we have documentation for this that was approved by our team management. ➔ level 3
- The service level of our Internet access is good enough for our purposes, and we have documentation for this that was approved by our team management. In the periodic review of our team it is checked if this Internet access resiliency is sufficient. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.8 T-8: Incident Prevention Toolset

Question

Does your CSIRT have a collection of tools aimed at preventing incidents from happening in their constituency? The team either operates or uses these tools, or has access to the results generated by them. Examples are IntelMQ, TARANIS, IPSs (Intrusion Prevention Systems), virus scanners, spam filters, port scanners.

Answers
- We are a purely incident coordinating/handling team not involved in prevention. ➔ level -1 : will be omitted from scoring
- We never really discussed this. ➔ level 0
- We have such tools, but have not listed or documented them. ➔ level 1
- We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have such tools, have documented these and this was approved by our team management. ➔ level 3
- We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.9 T-9: Incident Detection Toolset

Question

Does your CSIRT have a collection of tools aimed at detecting incidents when they happen or are near to happen? The team either operates or uses these tools, or has access to the results generated by them. Examples are MISP, AbuseHelper, IntelMQ, IDSs (Intrusion Detection Systems), quarantine nets, netflow analysis tools – but also your tools to receive incident reports (phone, e-mail).

Answers

- We never really discussed this. ➔ level 0
- We have such tools, but have not listed or documented them. ➔ level 1
- We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have such tools, have documented these and this was approved by our team management. ➔ level 3
- We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.3.10 T-10: Incident Resolution Toolset

Question

Does your CSIRT have a collection of tools aimed at resolving incidents after they have happened? The team either operates or uses these tools, or has access to the results generated by them. Essential elements of this toolset are the hardware your team uses (computers, routers/switches, storage etc.) and your connectivity (which may include separate Internet connections for contingency and/or testing purposes). Other examples are forensics toolkits, your incident tracking system (RTIR, OTRS etc.), but also bear in mind that all team members need to have easy access to very basic tools such as whois, traceroute, IP#-to-CSIRT resolution tactics (IRT object, TI and FIRST information, etc.).

Answers

- We never really discussed this. ➔ level 0
- We have such tools, but have not listed or documented them. ➔ level 1
- We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have such tools, have documented these and this was approved by our team management. ➔ level 3
- We have such tools, have documented these and this was approved by our team management. In the periodic review of our team it is checked if these tools are sufficient to meet our requirements. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better

- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4 P – Processes parameters

3.4.1 P-1: Escalation to Governance Level

Question

Does your CSIRT have a process to quickly and as directly as possible inform/alert the upper management of your team's constituency, when an incident or threat occurs that has both high urgency and impact (the latter two probably based on your Incident Classification, see O-8)? If the constituency is external to your host organisation, and exists of more independent organisations, you need to be able to escalate to all of them. Bear in mind that this kind of escalation by its nature needs to be effective at all times, not just in business hours. And in order to be effective, the escalation chain needs to be very short.

Answers

- We never really discussed this. ➔ level 0
- We have an informal way of escalating, but this was never written down. ➔ level 1
- We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written escalation process approved by our team management. ➔ level 3
- We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 3 or better
- Intermediate: level 3 or better
- Certifiable: level 4

3.4.2 P-2: Escalation to Press Function

Question

Does your CSIRT have a process to quickly and directly inform your host organisation's press office, when an incident or threat occurs that has both high urgency and impact?

Answers

- We never really discussed this. ➔ level 0
- We have an informal way of escalating, but this was never written down. ➔ level 1
- We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written escalation process approved by our team management. ➔ level 3
- We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.3 P-3: Escalation to Legal Function

Question

Does your CSIRT have a process to quickly and directly inform your host organisation's legal office, when an incident or threat occurs that has both high urgency and impact?

Answers

- We never really discussed this. ➔ level 0
- We have an informal way of escalating, but this was never written down. ➔ level 1
- We don't have a formal written escalation process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written escalation process approved by our team management. ➔ level 3
- We have a formal written escalation process approved by our team management. In the periodic review of our team it is checked if this process has been used appropriately and how it worked. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.4 P-4: Incident Prevention Process

Question

Does your CSIRT have a process describing the activities aimed at preventing incidents, including the use of the related toolset (see T-8)? This includes the adoption of pro-active services like security awareness raising and the issuing of threat/vulnerability/patch advisories.

Answers

- We are a purely incident coordinating/handling team not involved in prevention. ➔ level -1 : will be omitted from scoring
- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better

- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.5 P-5: Incident Detection Process

Question

Does your CSIRT have a process describing the activities aimed at detecting incidents, including the use of the related toolset (see T-9)? Be reminded that receiving incident reports by phone or e-mail is part of incident detection. Note that frequently P-5 and P-6 are combined in one process, often called incident handling or incident management process.

Answers

- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.6 P-6: Incident Resolution Process

Question

Does your CSIRT have a process describing the activities aimed at resolving incidents, including the use of the related toolset (see T-10)? Note that frequently P-5 and P-6 are combined in one process, often called incident handling or incident management process.

Answers

- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.7 P-7: Specific Incident Processes

Question

Does your CSIRT have a process describing how the CSIRT handles specific incident categories, like phishing, DDoS or copyright issues? This kind of extra information is especially useful for incident types that can be mission critical (e.g. DDoS), or for incident types where a standard way of dealing with them has been developed (e.g. copyright issues). Note that P-7 may be already part of P-6.

Answers

- We treat all incidents the same way, no additional info is available for different types of incidents. ➔ level 0
- We have some standard ways of dealing with different incident types, but have not documented this. ➔ level 1
- We don't have formal written specific incident processes, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have 1 or more formal written specific incident processes approved by our team management. ➔ level 3
- We have 1 or more formal written specific incident processes approved by our team management. In the periodic review of our team it is checked if these process(es) work(s) as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.8 P-8: Audit/Feedback Process

Question

Does your CSIRT have a process describing how the set-up, human aspects, operations and processes of the CSIRT are reviewed by self-assessment, and by audits, and a subsequent feedback mechanism? Those elements considered not up-to-standard should be considered for future improvement.

Answers

- We never really discussed this. ➔ level 0
- We do have reviewing, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management and by higher management, and higher management is leading in this. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 4

3.4.8.1 P-9: Emergency Reachability Process

Question

Does your CSIRT have a process describing how to reach the CSIRT in cases of emergency? Who are the key stakeholders for this process (your constituency? and/or only those CSIRTs who share a trust circle with your team, like TI Accredited teams, FIRST members, or CSIRTs network teams?) and do they have access to this process? Note that e.g. for TI Accredited teams, emergency reachability is defined as one of the parameters.

Answers

- We never really discussed this. ➔ level 0
- Key stakeholders know how to reach us in cases of emergency, but we have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes and made it available to our key stakeholders. Our management has not formally approved this. ➔ level 2
- We have a formal written process available to our key stakeholders and approved by our team management. ➔ level 3
  (Note that published information, either inside the constituency or in some external database (e.g. TI) also counts as level 3.)
- We have a formal written process available to our key stakeholders and approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 3 or better

3.4.9 P-10: Best Practice Internet Presence

Question

Does your CSIRT have a process describing (1) the way in which generic, security related mailbox aliases @org.tld are handled by the CSIRT or by parties who know when what to report to the CSIRT – (2) the web presence, and (3) any social media presence ?

Minimum requirement:

(1) The handling of the following mailbox aliases (from RFC-2142 and best practice) is secured in such a way that the handlers either are part of the CSIRT **or** know the CSIRT, what it is for, and how to reach it when needed:

Security: security@ ; cert@ ; abuse@
E-mail: postmaster@
IP-numbers & domain names: hostmaster@
WWW: webmaster@ ; www@

(2) Some form of web presence for the CSIRT, at least internally. That presence must at least explain what the CSIRT is for, who it is for, and how it can be reached and when. Additional *recommendations* are (a) to link rfc-2350 from that presence, and (b) to enable a slash-security page, that is a page like www.org.tld/security , which can serve a wider security purpose than just the CSIRT.

(3) Social media presence is optional, but needs to be considered. Twitter, Facebook etcetera.

Answers

- We never paid much attention to this. ➔ level 0
- We have several of these taken care of, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 2 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.10 P-11: Secure Information Handling Process

Question

Does your CSIRT have a process describing how the CSIRT handles confidential incident reports and/or information? This also has bearing on local legal requirements. Note: this process should also support the use of TLP, the information sharing Traffic Light Protocol.

Answers

- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 3 or better

3.4.11 P-12: Information Sources Process

Question

Does your CSIRT have a process describing how the CSIRT handles the various information sources available to the CSIRT (as defined in the related tool, if available – see T-2)?

Answers

- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1

- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.12 P-13: Outreach Process

Question

Does your CSIRT have a process describing how the CSIRT reaches out to their constituency, not with regard to incidents but regard visibility of the CSIRT, awareness raising and "PR"? This process should include all forms of such outreach, varying from webpages, via newsletters, advisories to seminars, workshops, trainings etcetera.
Note that e.g. for national CSIRTs this process would also be about reaching out to the various sectors in society/economics served by the team.

Answers
- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 4

3.4.13 P-14: Reporting Process

Question

Does your CSIRT have a process describing how the CSIRT reports to the higher management and/or the C(I)SO of their host organisation, i.e. internally?

Answers
- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2

- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management and by higher management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 2 or better
- Intermediate: level 3 or better
- Certifiable: level 4

3.4.14 P-15: Statistics Process

Question

Does your CSIRT have a process describing what incident statistics, based on their incident classification (see O-8), the CSIRT discloses *to their constituency and/or beyond*? Note that is *not* about statistics in management reporting: that is covered by P-14.

Answers
- We have made an explicit choice only to report statistics internally, not to our constituency or beyond. ➔ level -1 : will be omitted from scoring
- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:
- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.15 P-16: Meeting Process

Question

Does your CSIRT have an internal meeting process, describing *at least* how often the team meets?

Answers
- We never really discussed this. ➔ level 0
- We do meet regularly, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

3.4.16 P-17: Peer-to-Peer Process

Question

Does your CSIRT have a process describing how the CSIRT works together with peer CSIRTs and/or with their "upstream" CSIRT? Note that an "upstream" CSIRT does not exist for many leading teams, like national teams, or corporate teams; they will usually have "peers" though, inside their sector – for a national team the natural peers would be other national teams.

Answers

- We never really discussed this. ➔ level 0
- We know how we do this, but have not documented this. ➔ level 1
- We don't have a formal written process, therefore we wrote something for our own purposes. Our management has not formally approved this. ➔ level 2
- We have a formal written process approved by our team management. ➔ level 3
- We have a formal written process approved by our team management. In the periodic review of our team it is checked if this process works as intended. ➔ level 4

Proposed demands for CSIRTs network maturity steps:

- Basic: level 1 or better
- Intermediate: level 2 or better
- Certifiable: level 3 or better

4. Peer Review Methodology

The self-assessment proposed above serves many purposes, most of all to learn about its own capabilities and capacities. But its values are directed inwards, not outwards. Therefore, the main question that other CSIRTs will have about any one team is still un-answered: How mature is the team I am looking at?

Right now, only one Certification scheme is available, provided by the Trusted Introducer service based on SIM3, which can answer this question objectively based on the long-term experience of the auditors. But there should be another alternative available that can answer the same question, maybe not to the same degree, but good enough for practical purposes. Such purposes might be in the context of the NIS Directive or the collaboration of teams in a specific trust circle like CSIRTs network.

To achieve this, a peer review methodology was designed, which is explicated below. The peer review methodology is defined based on four leading principles that can be described by asking the following questions:

1. Who carries out a peer review?
2. What specifically is reviewed and to which degree?
3. How are the results documented?
4. Which results are communicated to whom?

These four principles are detailed below, and the questions answered.

4.1 Who carries out a peer review?

Obviously, just by the name of it, only peers can carry out such reviews. The reviewer needs to have significant working knowledge of the context of the team and their working relationships, as well as the overall setup of such teams. The team to be reviewed has this knowledge and could therefore propose 3 to 5 potential reviewers to ENISA who could serve as intermediary in this “match making” process.

This means, that the potential reviewer will come from the same trust circle(s) and must be a senior representative of their own team with at least 5 years of practical experience working in these trust circles and as part of an operational CSIRT. Alternatively, the team can request that an ENISA CSIRT-relations senior expert be the reviewer.

Ideally, the peer reviewer has hands-on experience with the adoption of the SIM3 model, e.g. because (s)he worked or works for a team that was Certified by the Trusted Introducer.[8]

4.2 What is exactly reviewed to which degree?

A peer review of *all* SIM3 parameters would require too much effort on the side of the peer reviewer. To review only one or two of the four main areas – organisation and human issues for example – would

[8] The Open CSIRT Foundation will start to provide trainings for SIM3 assessors in the autumn of 2017. Such a training specifically for reviewers inside the CSIRTs network could help improve the peer review process.

reduce the effort required for the peer review, but not cover all important topics. Therefore, it is recommended to focus the peer review on the following two items:

1. Has the team representative provided the results (completed self-assessment for all SIM3 parameters) to the peer reviewer and signed it? This ensures that the peer reviewer has a good foundation to go from and can base their further actions on the self-assessment results. The signature signifies compliance with the model and principles adopted (SIM3 tuned for CSIRTs network usage).

2. The peer reviewer will always discuss and review the following parameters:
   Organisation: O-1, O-4 and O-10;
   Human: H-1, H-2, H-4, H-5, H-6, H-7;
   Tools: T-2, T-4, T-5;
   Processes: P-1, P-6, P-9, P11, P-17.

3. Based on the self-assessment results the peer reviewer will discuss and **check** all those parameters, that are declared as "level 4" by the team representative. **Checking** means that there needs to be substantiation for these parameters which can be reviewed. This will be further explained below.

To explain the reasoning behind #2 and #3 above, we will shortly look at the SIM3 levels again. SIM3's real life applicability has been achieved by adopting a unique set of levels, valid for *all* parameters all categories:

Level	Explanation
0	Not available / undefined / unaware
1	Implicit (known/considered but not written down, "between the ears")
2	Explicit, internal (written down but not formalised in any way)
3	Explicit, formalised on authority of the CSIRT management ("rubberstamped" or published)
4	As 3, but regularly and explicitly assessed on authority of governance levels above the CSIRT management

So basically, with the signature of the team management all parameters can be declared up to "level 3". This can be ensured by her/him, given that there is a written document that can be signed. While it can

be certainly checked whether such written documents really exist (as is done in TI Certification, for example), this is not needed inside a closed trust circle.[9]

The reason to still always discuss and review a number of parameters (as mentioned under #2 above) is that these parameters are seen as so important in the light of the CSIRTs network, that it is both important and beneficial for all teams involved to share ideas on those and gain common understandings. "Reviewing" in this case means, that the peer reviewer accepts the declaration of the team management up to "level 3" but will discuss what this means in the practice of the team, and compare it with the practices of their own team (and possibly others that they may have reviewed).

It also follows from the table above that specifically those parameters that have been declared as "level 4" must be checked by means of reviewing substantiation. Here too, however, the discussion element is essential for gaining better and common understanding.

Still the question will be, what specifically should be checked then, and to which degree, for those SIM3 parameters that will have been declared as "level 4". Such parameters require a governance influence **above the CSIRT management**. Therefore, the peer review needs to focus here on the existence of those higher governance levels, the rules as defined by national law or organisational policies, and the execution of the "regular and explicit assessment" on authority of those governance levels.

So what the peer reviewer needs to identify and check is the existence of any such process and evidence that this is indeed "above" the CSIRT management. It is important to note again that this does not include the checking on any **results** of such processes in the past or current. A description of the process and evidence, like a formal statement of an overseeing body, would be sufficient.

4.3 How are the results documented

The documentation of the peer review results is relatively simple:

a) It must contain a reproduction of the signed self-assessment provided by the team representative, which may include the team's own comments on all SIM3 parameters;
b) A summary of review findings for the parameters O-1,4,10; H-1,2,4,5,6,7; T-2,4,5 and P-1,6,9,11,17;
c) A summary of review findings for all SIM3 parameter declared as "level 4", plus an explicit confirmation that in the eyes of the peer reviewer these are correctly declared as "level 4;
d) The date of the documentation and name of the peer reviewer as well as the signature.

4.4 Which results are communicated to whom?

As the peer reviewer collects all details and insights necessary to produce the documentation, a draft version shall be produced and presented to the team representative for review. If any interpretation needs to be discussed, this would be the point in time to bring it up with the peer reviewer before concluding the review.

[9] If – at some later point in time – it might become clear, that one or more of such documents may never have existed, this would remove all trust in the team. In addition, it can be assumed, that based on such peer pressure and the dependence of the team to work within these trust circles, no team will jeopardise their trust-status in the community by foul-play.

After the final documentation has been produced, the documentation is sent to ENISA for further processing.

This research and proposed solution on CSIRT maturity assessment is tailored for the NISD CSIRTs network needs and requirements. The outcome of this document should be further implemented within this Network.

5. Conclusions

The NISD aims at creating a CSIRTs network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". Each Member State shall designate one or more CSIRTs that shall comply with a set of defined high-level requirements.

ENISA's 2016 report *Challenges for National CSIRTs in Europe in 2016 : Study on CSIRT Maturity* concluded the following, in short:

1. A sustainable and implementable approach towards assessing and improving maturity is best based on a measurable set of quantities, or parameters. The SIM3 model as is commonly used in Europe serves as an excellent basis for this, with some additions based on especially the NIS Directive.
2. The three-tier approach towards maturity steps that ENISA adopted in the past can be used to define three steps when adopting the SIM3 maturity model to assess CSIRT maturity: basic, intermediate and certifiable tailored to the needs of the CSIRTs network.
3. An explicit definition of those three steps for the benefit of the NISD CSIRTs network has been proposed in the report. Basic step already allows successful co-operation between teams on incident handling, the higher steps are needed to allow the members of the CSIRTs network to interact on all levels, including pro-actively. The Certifiable step has been defined at the level of the existing CSIRT Certification scheme in Europe, which means that certification is within reach once that maturity level has been reached.
4. A validation process based on self-assessments and peer-reviews has been suggested in the report, pending further explication.
5. By adopting this approach, the NISD CSIRTs network will have immediate access to a clearly defined CSIRT maturity improvement process that is both implementable and sustainable. A growth path has been suggested in the report that asks teams to reach basic step within one year, intermediate two years later and certifiable another two years later.

The report presented here is a further explication of point 4. above, focusing on two important aspects of the CSIRT maturity improvement process:

1. Self-assessment survey. A survey with questions and answers for all the SIM3 parameters was delivered here, which makes it considerably easier for any team to self-assess their maturity in the terms of SIM3 parameters. The survey is complete with a mapping to the proposed CSIRTs network maturity scale (with the steps basic, intermediate and certifiable), so that members of the CSIRTs network who use the survey can self-assess their maturity on that scale.

2. Peer review methodology. A methodology for how to do peer reviews inside the CSIRTs network was delivered here, complementary to the self-assessment approach and intended as a form of intra-community mutual support aimed at further enhancing all teams' maturity. The proposed peer review approach is a flexible one, that is expected to suit the needs of all teams involved.

With all these building blocks in place, the next recommended steps are:

1. Discussion inside the CSIRTs network on content and application of both maturity studies. (May – June 2017)

2. A small scale pilot application, involving up to 3 volunteer teams of varying maturity to do self-assessments and 1 TI-certified team as peer reviewer. (September-November 2017)

3. Revising the models used based on the pilot outcomes. During the whole process it is recommended to stay in close touch with ENISA about recommendations on CSIRTs capabilities and maturity and also with the (not-for-profit) Open CSIRT Foundation, who have assumed the SIM3 stewardship role in October 2016, to make sure that the SIM3 related developments are synergetic. (November-December 2017). Additionally, it is seen as highly recommendable to synchronise with the CEF CSP project that is being rolled out from 2017-2019 for the CSIRTs network community, as this project has budget and plans to organise a series of trainings in 2018 that aim at increasing the CSIRT maturity level, as a boundary condition for successful take-up of the CSP services – and as the thinking of the project consortium on fostering maturity has a high degree of synchronicity[10] with the ideas presented in this report, a win/win situation is within reach.

4. Decision for roll-out inside CSIRTs network. (January 2018)

5. Roll-out. (Timing to be decided in step 4.)

[10] This observation is based on communications with representatives of the CEF CSP project consortium.

References

[1] Open CSIRT Foundation: https://www.opencsirt.org/ [2] http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement/
[3] The ENISA report *Challenges for National CSIRTs in Europe in 2016 : Study on CSIRT Maturity* (2016) has been made available to the potential members of the CSIRTs network
[4] https://www.trusted-introducer.org/SIM3-Reference-Model.pdf (2009)
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-01-17-598-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-223-3
DOI: 10.2824/35988