SIM3 v2 interim – Security Incident Management Maturity Model

Full Standard

1 January 2023

Don Stikvoort, Klaus-Peter Kossakowski, Mirosław Maj

Abstract

Including the SIM3 standard descriptions this SIM3 manual also contains the further guidance developed for sim3-check.opencsirt.org. Together, document and tool provide the first comprehensive guide helping not only SIM3 auditors but also every person that would like to conduct a guided self-assessment.

Acknowledgement and Justification

This SIM3 v2 interim replaces the original SIM3, now called SIM3 v1, which was/is in use from 2008-2022 and was written up by Don Stikvoort – with the support of especially Klaus-Peter Kossakowski. For this original version, thanks are also due to the 2009-10 TF-CSIRT certification WG (Serge Droz, chair, Gorazd Bozic, Mirosław Maj, Urpo Kaila, Klaus-Peter Kossakowski, Don Stikvoort) and to Jimmy Arvidsson, Andrew Cormack†, Lionel Ferette, Aart Jochem, Peter Jurg, Chelo Malagon, Kevin Meynell, Alf Moens, André Oosterwijk, Carol Overes, Roeland Reijers, Jacques Schuurman†, Bert Stals and Karel Vietsch† for their valuable contributions.

For the SIM3 v2 interim thanks are due to Vilius Benetis, Olivier Caleff, Andrea Dufkova, Kamil Gapinski, Maciej Pyznar and Edgars Taurins, for their valuable contributions. Note that this version is 'interim' and will see fundamental additions in 2024, especially for other types of security teams than CSIRTs, which were the focus of the original SIM3. Also note that for CSIRTs, the original SIM3 and SIM3 v2 interim are compatible, with the exception of the O-6 Parameter which was lacking in the original SIM3 but has been added to SIM3 v2 interim. All other differences between both for CSIRTs are not fundamental, but in fact a number of Parameter name updates, and numerous textual updates and improvements.

Starting Points

- The topic here is the Maturity of Security Incident Management (SIM) rather than just 'CSIRT' which by virtue of the name is about 'response' primarily. SIM has four major pillars:
  - Prevention
  - Detection
  - Resolution
  - Quality control & feedback
- The primary scope here is cyber security incidents: incidents that are directly related to computers of all sorts, network appliances including IoT devices, networks and the information therein and conveyed thereon. One can however extend this scope, or narrow it down, often with no significant consequences for the model.

- For reasons of word economy, the term 'CSIRT' is used here to describe any SIM capability to which SIM3 is applied, whether team, service or function. 'ISIMC' Information Security Incident Management Capability is academically seen a better word than 'CSIRT' but the latter is widely known and therefore already rings all the right bells. The term 'CSIRT' is identical to the older name 'CERT', which is also commonly used.
- The copyright holders promote widespread use of this model. The copyright statement is intended to keep the model unified, i.e. avoid various versions being used at the same time, but also to avoid the creation of look-alike models that will only muddy the waters for the CSIRT community other than that, the copyright holders promote an 'open source' not-for-profit approach which will help improve this model and its applications. Anyone wishing to expand or improve or add to SIM3 are kindly requested to get in touch with the Open CSIRT Foundation (OF). Note that for-profit use is intended and promoted as well, but those wishing to do so are also requested to get in touch with the Open CSIRT Foundation (OCF) to create a synergetic approach. Both maturity and certification gain in meaning when there is an agreed on starting point. TF-CSIRT and their Trusted Introducer (TI) trust model have already adopted the original SIM3 in May 2010. This means that at that time over 200 European CSIRTs supported the use of SIM3. TF-CSIRT/TI has additionally based their Certification scheme on SIM3, which was launched in September 2010.
- Since that time, global fora such as FIRST, GFCE and ITU and trans-national fora like AfricaCERT, ENISA (and the EU CSIRTs Network), LACNIC, OAS and Trust Broker Africa have benefited from adopting SIM3, and several of them (especially ENISA) have contributed to its further development. Last but not least, a growing number of countries are adopting SIM3 for CSIRT development a few examples to show the geographical reach are Brazil, Japan, Slovakia and Vietnam.

Basic Elements

The SIM3 is built on three basic elements:

1. Maturity Parameters
2. Maturity Quadrants
3. Maturity Levels

The *Maturity Parameters* are the quantities that are measured in regard to maturity over 40 exist and they are detailed below.
Each Parameter belongs to one of four Quadrants - the Quadrants are therefore the main four categories of Parameters:

- O - Organisation
- H - Human
- T - Tools
- P - Processes

These four Quadrants have been chosen in such a way that the Parameters in there are as mutually independent as possible.

Measuring the Maturity

What we really measure are the Levels for each Parameter. A desirable simplicity of the SIM3 has been achieved by specifying a unique set of Levels, valid for all of the Parameters in all of the Quadrants:

- 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 head or above (rubberstamped or published)
- 4 = explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)

To make these five Levels even clearer, we offer a more informative description here:

- 0 : This Level is mostly only met with teams who are fairly novice, as it means that the team members have not even been thinking yet about the Parameter in question. If during an assessment or audit all attendants produce blank looks when a Parameter is mentioned, this is probably a candidate for level 0. When a team starts actively discussing a Parameter, there is a high likelihood of it moving to Level 1 fairly soon.

- 1 : This Level is typically encountered with novice teams but, for some Parameters, also with experienced teams where a few experts know how to do things but never took the trouble of writing them down. When doing an assessment or audit and a Parameter at Level 1 is encountered, it is worthwhile asking a few team members to explain how they think about that Parameter. Chances are that the explanations will be different enough to convince the team as well as the team head that it is a good idea to actually write the content for that Parameter down, as to increase consistency within the team and also making it easier to get new team members up to speed.

- 2 : This Level is typically encountered when teams have internal information systems of a more informal type. Like a team-wiki, or shared site or similar. It is strongly recommended to have a facility like that for any CSIRT as it allows an easy way to bring the most important processes, tools (and manuals) and policies under the direct attention of those doing the incident management work. A wiki-style approach has the added advantage of allowing hyperlinks, thus enabling the internal information to be easily structured and interconnected: example, T-2 is the information sources list, and from that list you could easily point at the process(es) relevant for those various sources and those processes comprise the P-12 Parameter.
  There are also some other cases that can lead to a Level 2 score, like for instance when some tool used by the team holds information relevant for one of the Parameters, but this information has not been ratified by the team head. Example: the incident tracking system (T-4) of the team will most likely have some kind of incident classification scheme (O-8) on board but that will be in the form of a dro-pdown choice: when that drop-down list has not been formally approved by the team head, the O-8 Parameter scores at level 2.
  Going back to the wiki-style approach: the typical character of that approach is that various team members can write texts and fit them in and even when consensus among team members about such texts will come into existence after continued use (and adaptation, again wiki-style), this is still level 2, as there is no formal approval by the team head (or above). Level 2 is certainly valid to begin documentation with, but for

most information it is advisable that, at some stage, what has come to be the consensus is also recognised as such and supported by the team head leading to level 3.

- 3 : This Level applies for any Parameter where the subject matter of that Parameter has been formally and explicitly (in "writing") approved by the team head (or above). To mention a few of the most common situations for Level 3:
  - The subject matter is part of policy or process documents on the team level, authorised by the team head: these comprise the most simple and direct case, however the risk inherent in separate documents is that if there are too many of those the overview is lost and it can become a separate paper reality, rather than part of the day-to-day procedures of the team. Therefore, it is important to integrate such documents in team operations and information systems to ensure that team members actually know and use them. For instance by integrating them into a team-wiki or similar. In addition, it is strongly recommended to use an expiry and maintenance system for team-internal documents.
  - Relevant policy (or process) documents authorised on a governance level higher than the team head: these are automatically also valid for the team head and the team; however it is essential that they are embedded into the team operations and information systems as to ensure that the team members actually know and use them.
  - Wiki-style level 2 information/pages/documents that are "upgraded" to become level 3: this of course requires explicit (visible) authorisation by the team head of such "pages". It is currently not YET demanded by SIM3 but it is STRONGLY recommend to go one step beyond this and not just do authorisation, but also include some system of expiry and maintenance for such pages. Some wiki-types have facilities or plugins to make that easier.

- 4 : This Level implies Level 3 plus an important addition that ensures that the Parameter in question is no longer just an internal matter of the team, but has the active attention of some higher governance level, above the team head. There needs to be evidence of this, and the evidence must include the following:
  1. There must be a process of checking, assessing or auditing of this Parameter on the authority of a higher governance level.
  2. This process must be followed regularly. There is currently NOT YET a set rule for this in SIM3, but as best practice "regular" means at least once every 2 years, and usually once per year.
  3. The process must be "active", which means that there is a feedback mechanism towards the team head (and team) in addition to the process of checking and reporting on that. This feedback mechanism is meant to ensure that there is communication about the Parameter between team (head) and higher governance levels.

  This level 4 mechanism is meant to ensure that (a) the higher level of governance is actively aware of some of the crucial aspects of the CSIRT and how it functions in real life, and (b) as a consequence, to enable constructive communication between higher governance level and the team in order to enable improvements: clearer policies, better tools and processes, more people, better trainings and education, etcetera.
  The evidence for level 4 is not always clear-cut. The clearest cases are the following two:

- When the topic of Parameter is formally and unambiguously part of a country's cyber (security) legislation that Parameter automatically scores level 4, because it is assumed that the system of legislation and the checks and balances associated with that are more than sufficient to warrant a level 4. It is however important to note here that the mere mentioning of something in the law even if clear and unambiguous still requires the team to implement this internally as to be able to effectively “make the law work”. So this still requires documentation inside the team for such aspects, embedding in a team information system (e.g. team wiki), integration in internal training, etcetera.
- When there is a team organisational framework or charter (Parameter O-10) or a “team handbook” it is strongly advised to have a paragraph there about the assessments/audits for the team, which is essentially the P-8 Parameter process. This should include internal team assessments (which on their own are not sufficient for level 4) but it should also address the process of auditing the team by a higher governance level or by an auditing department. As such higher level audits usually set their own rules, it is recommended to acknowledge their independent position, but to request a minimum set of aspects (which could directly be translated into SIM3 Parameters) on which the team wants to be audited. Most of the O-Parameters could be included there, plus optionally some others, like H-2, P-1 and P-2.

In other cases, it is often harder to find clear evidence for the Level 4 character. For instance, when an auditing department does an extensive audit of the CSIRT every year, and they do use SIM3 as one of the controlling documents but no one has written down some minimum requirements for that audit. In such a case, alternative evidence can be a posteriori rather than a priori: meaning, simply ask for a few of those audit reports and see what is in there in order to be able to gauge whether it is reasonable to assume that certain SIM3 Parameters are indeed audited in the Level 4 way (including feedback to the team) and therefore there is reasonable substantiation to grant Level 4.

Such simplicity as is obtained by only 5 Levels for over 40 Parameters, is great in terms of ease of use and presentation but has its drawbacks too. This is especially noticeable in a few Parameters that, when you apply them in real life, are reluctant to be mapped onto a specific Level. However the advantages of this simplified scheme have shown since 2008 to far outweigh the few quirks encountered.

O - Organisation

With **Organisation** we refer to the ensemble of humans, resources, tools and infrastructures that work together in a planned manner. The objectives or aims of an organisation are directed by a set of specific strategic goals. As SIM3 focuses on the maturity of the management of security incidents, we need to distinguish between on the one hand strategic goals of the whole organisation, and on the other hand the (service) specific strategic goals related to that part of the organisation, that manages security incidents - commonly referred to as 'CSIRT'. The following 'O' Parameters are about the mandate, setup and services of that CSIRT, and the framework connecting all organisational aspects.

O-1 Mandate

Description: The CSIRT's assignment as derived from higher governance levels.

Your CSIRT needs to derive the justification for its existence, its assignment from some higher level of governance. This is called the CSIRT mandate. Ideally, the mandate comes from the highest governance levels in your specific environment. Sometimes it initially comes from a lower level, like the company's head of IT, or the leadership of a ministry. But preferably it comes from the highest levels, like the board of directors, or state government - and in the latter case it can also be anchored in legislation. Does your CSIRT have such a mandate?

O-2 Constituency

Description: Who the CSIRT functions are aimed at – the 'clients' of the CSIRT.

Your CSIRT's constituency is defined as the 'client base', the target group for who you do the CSIRT work. This constituency can be your own organisation or company - then it is said that your constituency is internal to your organisation. Your team can also have a constituency external to your own organisation, like for instance your country's universities when you serve the academic community, or a paying customer base, or all municipalities in your country. Does your CSIRT has a well defined constituency?

O-3 Authority

Description: the CSIRT is allowed to do towards their constituency in order to accomplish their role.

The authority of a CSIRT is what your team is *allowed* to do towards your constituency, so that you can fulfil your mandate. The authority is basically the powers that have been invested in your CSIRT. Some teams, like especially coordinating teams with an external constituency, have little powers, little authority and can perhaps only give advice to the constituency. Whereas others CSIRTs have the authority to enforce measures. What and how you can escalate, is also part of this. The whole purpose of this Parameter is to help ensure that the CSIRT has a clear and distinct description of their authority, which can serve as support in the back especially in crisis cases. It is important to realise that the authority of any CSIRT needs to come from higher governance, or else there will be no high-level support for the team in cases where the "power" needs to be used. For the example of a national CSIRT, if the national cyber security law provides clarity on their authority, so much the better U+2013 however, if the law is not very specific, then the CSIRT should make sure that the authority is defined more precisely, starting from the law. What authority does your team have?

O-4 Responsibility

Description: What the CSIRT is expected to do towards their constituency in order to accomplish their role.

The responsibility of a CSIRT is what your team is *expected* to do and perform towards your constituency, so that you can fulfil your mandate. Basically, the responsibility is a high-level version of what is detailed below in the team's services (O-5). In almost all cases a team has more responsibility than authority. An example: a team may well be responsible

for checking out if new threats could hurt their constituency, e.g. by doing non-interruptive port scans. But that's not to say that the team has the authority to go beyond "non-interruptive" scans - or indeed that if the team finds such vulnerabilities, that it can 'order' the constituents in question what to do: this will often be in the form of advice, not enforcement. A situation to avoid is where a team's authority is very small - but their responsibility very big. If the gap between O-3 and O-4 becomes too big, then a team is more or less expected to do many things, without having the power to actually make them work. That is a recipe for malfunctioning. There is a natural gap between O-3 and O-4 but it should not become too big. What responsibility does your team have?

O-5 Service Description

Description: Describes what the CSIRT service is and how to reach it.
*Clarification: An excellent starting point is FIRST's document 'FIRST Services Framework' that offers a comprehensive and structured definition of all the kinds of services that a CSIRT, ISAC or SOC (and to some lesser extent also PSIRT) can offer to their constituency. The way to use this framework is to start from your team's mandate – and the resources you have available – and then first select those services you **must** do in order to fulfil your mandate, and then to go on to those you would **like** to do (but probably don't have the resources for).*
{See https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1}
Minimum requirement: Contains the CSIRT contact information, service windows, concise description of the services offered and the CSIRT's policy on information handling and disclosure. Publicly available in English.

Whereas 'responsibility' is usually formulated as a high level form of expectations of your CSIRT, the description of your team's services are the way you further shape that into a concise list of services that you offer to your constituency, which will most likely include incident management/response, but also possibly vulnerability handling, malware analysis, awareness raising and potentially others. The original most popular listing of possible services to select from was the one from CERT/CC's CSIRT Handbook (also adopted by ENISA and Trusted Introducer). Since 2017, the FIRST CSIRT Services Framework has become a de-facto standard, because it offers a well structured and granular approach, especially in its latest 2.1 version. Whichever source you use, it is important to make a clear selection of those services you must or should offer based on your mandate, authority and responsibility - and taking into account the resources you have available.
It is essential to note here that the concept of O-5 is only to ask "have you defined your services towards the constituency, and what's the result". Detailing what those services should or should not include is up to the team, SIM3 makes no specific demands (although of course in other parameters it is assumed that every CSIRT at least deals with Incident Management as a service). The best way of using SIM3 and the FIRST CSIRT Services Framework as complementary standards is by looking at it like this: SIM3 serves as the overall maturity standard for the CSIRT, and can be visualised by a horizontal line with over 40 Parameters as tickmarks on that line. On O-5 a vertical line intersects the SIM3 horizontal line: that vertical line is the visualisation of the FIRST CSIRT Services Framework, which every team is strongly recommended to use to map their services portfolio in detail. All of this then leads to a list of services, and it is important to consider that at least your constituency needs to have access to this list, including your team's contact information and service windows. It is strongly advised to use RFC2350 as a standardised way to publish a high-level list of their services, contact info and service windows even to the Internet at large, as for any CSIRT it is important that it is known how to reach them, as

they take responsibility for (part of) the security of their constituency, which is part of the wider Internet - when adopting RFC2350 make sure to have an English version publicly available (next to one in your native language). Does your team have a clear service description?

O-6 Public Media Policy

Description: Describes the CSIRT's policy on how to deal and interact with public media.
Clarification: If assessing/auditing a team based on SIM3 v1 (2008-2021), in which O-6 did not exist yet, omit this parameter from 'scoring'. This e.g. applies for the Trusted Introducer certification, as well as for GCMF v1/v2 assessments.

Your team needs to be able to interact with the press, and other public media. That is sometimes done together with a communications department, or press office - sometimes directly. This also depends on the kind of public media: dealing with the press is different from working with social media for instance. A public media policy will identify the various public media that are used, and how to deal with each of those. But this policy can also describe how to interact under specific circumstances, like for instance a big incident or crisis, an awareness raising campaign, or when e.g. the press wants to contact you instead of you reaching out to them. Does your team have such a public media policy?

O-7 Service Level Description

Description: Describes the level of service to be expected from the CSIRT.
Minimum Requirement: Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CSIRTs. For the latter a human reaction within two working days is the minimum expected.

When defining services that your CSIRT offers, it is useful to also set service levels for those services. What can your constituents expect of you in that regard? What can other CSIRTs expect of you? The simplest service level is some measure of the amount of time in which to send a first (human) reaction to an incoming incident report - SIM3 sets a minimum level here, it is mandatory to send a human reaction to peer teams within two working days (peer teams are those CSIRTs you have a well-defined relationship with, like being members of the same CSIRT cooperation or forum). Service levels can also be more detailed 'SLA' type demands, and can then also depend on the type, severity and priority of incidents (as e.g. defined in Parameter O-8, incident classification). Based on incident type and severity, different reaction times can be defined, but also e.g. the percentage of incidents that needs to be dealt with within a certain set amount of time. Does your CSIRT have a service level description?

O-8 Incident Classification

Description: The availability and application of an incident classification scheme to recorded incidents.

Incident classifications usually contain at least “types” of incidents or incident categories. However they may also include the 'severity' of incidents.
An incident classification scheme usually contains at least a list of technical incident categories to associate an incident or threat with, like whether it has the characteristics of

'spam' or 'root compromise' or 'DDoS' etc. A popular classification scheme of that type is ENISA's 'Reference Incident Classification Taxonomy'.
It is however recommended to also include in such a classification some measure of the potential severity (impact) of an incident or threat - and potentially also its assessed priority (as a high impact threat for instance can be low priority when its probability of happening any time soon is very low). Such more advanced ways of classifying incidents, coupled to the service levels defined in O-7, can help to deal in a structured way with higher incident loads. There are many ways of doing this, but it's advised to first see if the internal organisation already has some kind of severity/priority scheme for IT operations, and then possible adopt that. If you need to build one your own, the strong advice is to keep it simple, because all permutations you create may become visible in your O-7 and in various processes. Does your team have some kind of incident classification?

O-9 Participation in CSIRT Systems

Description: Describes the CSIRT's level of membership of a well-established CSIRT co-operation, either directly or through an "upstream" CSIRT of which it is a customer/client.
This is necessary to participate and integrate in the trans-national/worldwide CSIRT system(s).

With 'CSIRT systems' we mean well-established cooperations of CSIRTs, like in your country, sector, geographical region or worldwide. Your CSIRT can participate in those either directly, e.g. as member, or you may do so indirectly when you can make use of the services of an 'upstream' CSIRT that participates in such CSIRT cooperations. To be effective as a CSIRT, it is necessary to engage in this kind of participation, as the CSIRT community at large depends on this cooperation between teams. It is important to realise that this participation is crucial on various levels: inside a country for instance, it is necessary to create a CSIRT network, which includes the national CSIRT, plus CSIRTs defending the various parts of critical infrastructures, and also including the healthcare sector and research/education; in geographical regions it is also pragmatical and fruitful to come together (e.g. initiatives like or inside TF-CSIRT, APCERT, OAS, LACNIC, AfricaCERT, TBA, OiS-CERT, ASEAN, and so on); and last but not least participation in global fora like FIRST, or in CSIRT initiatives taken by the GFCE, ITU, African Union and others. Where the focus of your team's participation will be, depends fully on the type and scope of your team. Does your team participate in such cooperations directly, or indirectly via an upstream CSIRT?

O-10 Organisational Framework

Description: Fits O-1 to O-9 together in a coherent framework document serving as the controlling document for the CSIRT.
Minimum Requirement: Describes the team's mission and Parameters O-1 to O-9 by either providing references to specific documents or combining the required details in a single document.

What we call a 'team charter' or 'organisational framework' for your CSIRT, is a consolidated controlling document for your team, describing who/what your team is, who you work for, what is expected of you and how this was mandated. This charter should include at least the SIM3 Parameters O-1 to O-9 and potentially a few more. Ideally, this charter has been approved by the same governance level that mandated your CSIRT. The great use of having such a consolidated write-up of O-10 is that this is indeed the high-

level “charter” of any team the controlling document describing all the foundational issues for which the approval of higher governance is needed, and can serve as a reference from then on for the functioning of the team, for audits, etcetera.
O-10 is not necessarily only ONE document, though it is generally beneficial to have the foundational O-Parameters described in one document. Your team's charter is normally an internal document - therefore RFC2350, which is basically meant as public service description of your team, is not suitable as team charter - also RFC2350 is much more limited in scope than the charter is. If O-10 consists of more than one document, RFC2350 can be part of O-10 (but not all of it). For the example of national CSIRTs, most of O-10 can be in the national cyber security law - yet even then it can be very useful to re-iterate the O-10 related aspects in a charter on the team wiki, with the proper references.
There is one more variation that is worth mentioning: some CSIRTS decide to expand the charter document to comprise most or all SIM3 Parameters, thus creating what is often called a CSIRT handbook. The advantage of that approach is that all Parameters are described in one consolidated document - the flip side is that to get approval for such a handbook from the highest governance levels, means you also need to get high-level approval for all the more team-internal items like tools and processes, which may make version management more of a challenge. Does your CSIRT have such a charter?

O-11 Security Policy

Description: Describes the security framework within which the CSIRT operates. This can be part of a bigger framework, or the CSIRT can have their own security policy.

Your CSIRT is usually embedded in a host organisation. That host organisation will have information security and business continuity (BCM) policies, that will also apply to your team. Though often information security and business continuity are treated separately, it is more logical in the context of IT/cyber to have business continuity as an integral part of a good security policy, and that is the approach we take here. So when we say 'security policy' this includes such important aspects as 'availability', and how to get back to normal after disruptions - but the landscape is even broader than that, thought also needs to be given to site security and resilience, and workspace security and resilience. Two important notes must be made here:

- There are some other BCM related aspects that surface in other SIM3 Parameters. Specifically in H-2 which is about staff resilience, and T-5 to T-7 which are about the resilience of basic CSIRT tools.
- As a CSIRT, you often have IT/security/BCM requirements that differ from the normal ones - like you may want to be able to run tests without a firewall blocking those tests, or to receive e-mail without spam/malware filtering, you may want to place a honeypot somewhere, or you may need to be able to use encryption software like GPG or perhaps you need to have a dedicated Internet connections for back-up reasons, testing, etcetera. Such special CSIRT requirements often make it necessary that additional to your host's organisation security policy, your CSIRT also has its own security policy (again including the aspect of BCM). Of course when you are a stand-alone CSIRT without host organisations (meaning: you are your own host organisation), the same arguments apply.

Does your CSIRT follow a set security policy, or security policies (including BCM aspects), whether your own and/or of your host organisation?

H - Human

With **Humans** we refer to the people working together to provide the services described in the Organisation area and satisfy the mandate. All people contributing to the goals of the (CSIRT) organisation that manages security incidents, require a technical and/or management oriented education with considerable on-the-job training plus additional training for more detailed expertise like malware analysis or forensics. The 'H' Parameters in this area are about the factors of importance in regard the most important factor in any CSIRT: the human 'capital' of the people working there.

H-1 Code of Conduct/Practice/Ethics

Description: A set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work.
Clarification: E.g. the TI CCoP or EthicsFIRST. 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.
{See https://www.trusted-introducer.org/TI-CCoP.pdf and https://ethicsfirst.org}

Does your CSIRT provide guidance, guidelines or sets of rules for its team members on how to behave professionally, in an ethical manner? Often called a 'Code of Conduct (CoC)' a 'Code of Practice (CoP)' or 'Ethics guideline', it can provide golden rules on confidentiality, trustworthiness, and other key human qualities expected from CSIRT team members. Note that in most cases the CSIRT's host organisation will have some kind of ethics code, but such codes are of a generic nature and have nothing to do with the specific work that the CSIRT does - therefore such generic codes are not valid to satisfy H-1. The CSIRT regularly deals with highly sensitive data, and communicates not just inside the host organisation, but also outside. Also, responsible behaviour of CSIRT team members is not limited to the work context, but also relevant in private circles where security is concerned. The Trusted Introducer CSIRT Code of Practice (TI CCoP) can be used as CoP baseline, as it was written specifically for CSIRTs; another excellent starting point is 'EthicsFIRST' made by FIRST, which has its own website. That said, specific CSIRT cooperations, or even specific teams, can have good reasons to make their own code. Do note that proper alignment with the security policy (O-11) is always necessary. Does your team support such a code of conduct/practice/ethics?

H-2 Staff Resilience

Description: How CSIRT staffing is ensured during illness, holidays, people leaving, etc.
Minimum Requirement: Three (part-time or full-time) CSIRT members.

Does your CSIRT have enough staffing to deal with planned or unexpected team members' unavailability? Such cases include illness, holidays, quitting of job ... Depending on the services offered (O-5) and the service levels (O-7), the number of team members will vary, but ensuring availability in times of crisis must be anticipated. Based on the list of the bare minimum services to deliver in all contexts, it is commonly agreed that three (part-time) team members is an absolute minimum for any team. Note that staff resilience is also an

aspect of Business Continuity Management (BCM), which also appears in the O-11, and T-5 to T-7 Parameters. What about the staff resilience of your team?

H-3 Skillset Description

Description: Describes the skills needed on the CSIRT job(s).
Clarification: An excellent starting point is FIRST's document 'CSIRT Roles and Competences' that starts from the FIRST Services Framework, and then works towards the skills/competencies needed for the various roles that bring all kinds of services to the constituency alive.
{See https://www.first.org/standards/frameworks/csirts/csirt_roles_competences}

Does your CSIRT have a description of the skills needed on all CSIRT team position(s)? All positions must be defined, and include a description of expected team members' skills: this includes technical, knowledge, experience, and soft skills - e.g. communication, team spirit, working under stress, etcetera. Staff development planning (see H-4) can help to fill the gaps in team members' skills. Has your team described the skillsets needed?

H-4 Staff Development

Description: Staff development policy, to facilitate the training of new team members and improve the skills of existing ones.

Does your CSIRT have a policy for the professional development of their staff? This parameter is about staff development as a whole, probably including but not limited to a training plan for new team members, personal development planning and a catalogue of trainings for existing team members, team building/education schemes, etcetera. Staff development should enable new as well as existing team members to improve their skills, and meet the targets defined in the skillset (H-3) that applies to their job position. Staff development can take the shape of on-the-job-coaching, internal or external trainings, but also includes peer mentoring schemes (colleagues helping each other to get better at their jobs), management evaluation interviews, and team meetings and internal workshops. Note that H-5 and H-6 zoom in on two important aspects of staff development, important enough to warrant separate parameters, but H-4 is the overarching policy. Does your team have such a staff development policy?

H-5 Technical Training

Description: Programme to allow staff to get job-related technical training - like TRANSITS, ENISA CSIRT Training, or commercial training programs (CERT/CC, SANS, etc.)

Does your CSIRT provide team members with a programme of (external and/or internal) trainings they can take in order to improve their technical or 'hard' skills (as opposed to the 'soft' skills that are the subject of H-6), in order to meet the technically oriented targets asked for in the skillset (H-3) that applies to their job position. This includes new topics or technologies, future security directions, and technological deep dives. CSIRT-related trainings are TRANSITS, trainings delivered by ENISA or FIRST or any of the regional cooperations, or commercial training programs - e.g. CERT/CC, SANS, ... Note that H-5 should be part of H-4, but is so important that it warrants to be a parameter in and of itself. Does your team have such a technical training programme?

H-6 Soft Skills Training

Description: Programme to allow staff to get soft skills training, including especially (human) communication/presentation training.

Does your CSIRT provide team members with a programme of (external and internal) trainings they can take in order to improve their 'soft' skills (as opposed to the 'hard' skills that are the subject of H-6), in order to meet the soft skills oriented targets asked for in the skillset (H-3) that applies to their job position. All team members should be trained in such soft skills as team building, time management, working under stress, but especially also in (human) communication and presentation: The latter in order to better interact with clients, colleagues, managers, peers, local or foreign authorities, and sometimes also the press. This applies to all sorts of media - e.g. phone, chat, email, social media ... - and all types of communications - e.g. direct talks, meetings, presentations, advisory or report writing, blog posts, tweets and text messages. It applies to formal and informal communications, and not only to work activities, but sometimes also outside work (in compliance with the ethics code H-1). Also there needs to be attention for the fact that although 'normal' communication may cover 90% or more of all situations, crisis communication is different but equally important. Finally, those who may talk to the press, need additional training for that. Note that H-6 should be part of H-4, but is so important that it warrants to be a parameter in and of itself. Does your team have such a soft skills training programme?

H-7 External Networking

Description: Going out and meeting other CSIRTs. Contributing to the CSIRT system when feasible.

Does your CSIRT have a policy to send team members to CSIRT-related or cybersecurity-related meetings? This contributes to the national, sectorial, regional and/or worldwide CSIRT collaboration (the topic of O-9) - and those collaborations are essential for the success and effectiveness of the CSIRT community as a whole. Also, meeting in person creates the foundation for trust relationships with peers, and 'trust' is the cement of the CSIRT collaborations. Does your team have such a policy for external networking?

T - Tools

With **Tools** we refer to the collection of programs, applications, services, instruments and even simple pieces of equipment, that is used by the personnel that we discussed in the Human area, to reach the objectives and offer the services defined in the Organisation area. We specifically mean those tools that enable or improve the management of security incidents, improve it time-wise, quality wise, and/or with higher granularity, i.e. 'seeing' incidents that may before have gone unnoticed.

T-1 IT Assets and Configurations

Description: Describes the assets (hardware, software, OT, etc.) commonly used in the constituency, including their configurations, so that the CSIRT can provide targeted advice on these.

The availability of an up-to-date and sufficiently detailed list of what kind of computer/networking/OT resources the constituency uses, is very important for efficient security incident management. Such a list should include information about hardware, software and OT that the constituency members use. This should include relevant configurations: such more detailed information (including software versions in use) is necessary to deal with threats more effectively. Some organisations use IT assets management (ITAM) for this purpose, and maintain a configuration management database (CMDB). The CSIRT usually does not manage such assets/configuration lists, but does need to have access to them. Maintaining up-to-date and detailed information about the whole IT hardware/software and configuration landscape is challenging, and sometimes even impossible as in the case of coordinating CSIRTs with constituencies who 'run anything you can think of'. The fallback solution is to focus on only the most critical assets - and in such a case it could be the CSIRT itself who collects and maintains that information, in direct communication with their constituency. For national CSIRTs this task is even harder - and there especially a focus on CI(I) assets is necessary. Does your CSIRT have access to IT assets and configurations?

T-2 Information Sources List

Description: Where does the CSIRT get their vulnerability/threat/scanning information from.

A very important part of the CSIRT operations is the daily monitoring of all relevant information sources. These sources should include e.g. relevant social media accounts, that publish or distribute valuable information, or IT security related blogs or website services. Both time constrained information as well as longer term observations are important, not only for continuously adjusting the CSIRT operations but also for - and most importantly - the timely and effective reaction to current events. Of course this list needs to be maintained. Does your team have such an information sources list?

T-3 Consolidated Messaging System(s)

Description: When all CSIRT e-mail and other types of messages (signal, threema, wire etcetera) are kept in systems open to all CSIRT members, we speak of consolidated messaging system(s).

A CSIRT should organise its work in such a way that ensures the effective handling of incidents. This includes continuous information sharing between team members - in many cases also when they are not on duty. Also, incident reports will come in, and communication with other teams needs to be managed as well. E-mail and other types of messaging, like signal, threema, wire and other messaging tools, are the dominant communication mechanisms in most of these cases. Therefore the team must have resilient, high-quality, messaging system(s) that are consolidated (in the team's office, with good back-up facilities - or secure cloud based solutions) and all team members need access to it. It's of course possible to use the messaging system(s) of the host organisation, or a cloud service - however the security of such solutions needs to be taken into account - strong encryption of confidential data may be needed, or even obligatory. Does your CSIRT use consolidated messaging systems?

T-4 Incident Tracking System

Description: A trouble ticket system or workflow software used by the CSIRT to register incidents and track their workflow.
Clarification: RT(IR), OTRS, TheHive, trouble ticket systems in general.

A well-designed and tailored ticketing system is important for any CSIRT. In practice, when a team has to handle many incidents, it is near impossible to correctly manage all information and communication between team and involved parties, without such a tracking system. Only really small teams with a small number of incidents are able to manage the incident management process by using a very basic solution like a shared spreadsheet. In most cases, a dedicated solution is in need. Sometimes, the team reverts to using the host organisation's trouble ticket system - this is certainly possible, but similar to the e-mail case, confidentiality may again be a challenge, as most generic trouble ticket systems don't seem to have been designed with security in mind. Many CSIRTS have long term been using their own specific incident tracking systems - specifically open source solutions like RT(IR) (Request Tracker for Incident Response), OTRS (Open Source Ticketing Request System) or (of more recent date) TheHive. All these solutions are scalable and easy to use. Does your team use such an incident tracking system?

T-5 Resilient Voice Calls

Description: The voice call system available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.
Clarification: Voice calls include traditional phonecalls (mobile and fixed), plus voice calls using messaging tools - video can be included in voice calls. Mobile phones with all their many communication options are the easiest fallback mechanism for when a team's phone system is out of order.
Minimum Requirement: Fallback mechanism for the case of voice call system(s) outages.

Voice calls, be it traditional phone calls or via messaging tools, are a crucial communication tool for CSIRTs. It's part of how the CSIRT team members do their work, and manage incidents and perform their other duties. Therefore the uptime of the voice call tools available needs to support the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the voice call tools needs to be very high, so that any failure in those tools does not hinder the team's performance. In the case of voice calls, all such tools available to the team, like a classical 'landline', IP telephony, mobile phones, and messaging apps like signal, threema, wire and others, should be taken into consideration - mobile phones, with their multiple apps, often provide good means of resilience, especially when the services of more than just one mobile provider are used. A special, but rare, case is when a team has access to a (usually) national level protected communication system. What are your team's voice call facilities and are they sufficiently resilient for your purposes?

T-6 Resilient Messaging

Description: The messaging system(s) available to the CSIRT is/are resilient when their uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.

E-mail and other types of messaging are a fundamental communication tool for CSIRTs. It's part of how the CSIRT team members do their work, receive incident reports, manage incidents and perform their other duties. Therefore the uptime of the messaging tools

available need to support the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the messaging tools needs to be very high, so that any failure in those tools does not hinder the team's performance. In case of e-mail, there is also a reputation aspect here - when an incident reporter or another CSIRT receives an e-mail back indicating that your team's mail facility is not operational, this is bad PR. In the case of e-mail, a (hot) stand-by or fully resilient set-up is a possible (state-of-the art) solution - coupled to good back-up facilities for the mail storage, which will contain important and often sensitive incident data. For end-to-end secure messaging tools like signal, which is increasingly popular among CSIRTs because of its open-source strong cryptography, proper back-up schemes are important as by design there is no cloud storage. What are your team's messaging facilities and are they sufficiently resilient for your purposes?

T-7 Resilient Internet Access

Description: The Internet access available to the CSIRT is resilient when its uptime and time-to-fix service levels meet or exceed the CSIRT's service requirements.

Sufficiently fast and reliable Internet access is crucial to have for CSIRTs. Without that, the CSIRT can not normally function. Therefore the uptime of the Internet access needs to at least support and preferably exceed the team's service levels (Parameter O-7). Thus if a team has to be able to react quickly to incidents and solve them expediently, then the uptime of the Internet access needs to be very high, so that any failure there does not hinder the team's performance. Ideally, the CSIRT or its host organisation has a fully (even physically) redundant Internet access, but much less expensive solutions like having a back-up Internet access option (using a different technology as the normal one) may also be sufficient to meet your team's service level demands. As most teams depend on their host organisation for Internet access, it's useful that the team is qualified internally as one of the most demanding organisation units in regard Internet access. What are your team's Internet access facilities and are they sufficiently resilient for your purposes?

T-8 Incident Prevention Toolset

Description: A collection of tools aimed at preventing incidents from happening in the constituency. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: E.g. IPS, virusscanning, spamfilters, portscanning. If not applicable as for a purely co-ordinating CSIRT, choose N/A and the parameter will be omitted from 'scoring'.

This is about having a well defined and implemented set of tools that help with incident prevention. These tools are part of the first line of defence for the constituency. A CSIRT should clearly define its role regarding each of those tools. Some of such tools the team may run themselves, in other cases they may be the architect and a user - or they may only be a user of the tool, or have access to the results. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be closely involved in this area, or even decide about such tools. Examples of prevention tools: intrusion prevention systems, antivirus software, spam filters or vulnerability scanners. Does your team have a well-defined incident prevention toolset?

T-9 Incident Detection Toolset

Description: A collection of tools aimed at detecting incidents when they happen or are near happening. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: E.g. IDS, quarantainenets, netflow analysis.

This is about having a well defined and implemented set of tools that help with incident detection. These tools are like the ears and eyes of the CSIRT - they bring information about threats and incidents, from potential to exploited. A CSIRT should clearly define its role regarding each of those tools. Some of such tools the team may run themselves, in other cases they may be the architect and a user - or they may only be a user of the tool, or have access to the results. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be closely involved in this area, or even decide about such tools. Examples of detection tools: MISP, AbuseHelper, IntelMQ, network packet analysers - but also bear in mind that phone and e-mail are used for receiving incident reports and are thus detection tools too. Does your team have a well-defined incident detection toolset?

T-10 Incident Resolution Toolset

Description: A collection of tools aimed at resolving incidents after they have happened. The CSIRT operates or uses these tools or has access to the results generated by them.
Clarification: E.g. basic CSIRT tools including whois, traceroute etc; forensic toolkits.

This is about having a well defined and implemented set of tools that help with incident resolution. These tools support what is really core business for any CSIRT - the resolving of incidents. A CSIRT should clearly define its role regarding each of those tools. Because these tools are so mission critical, the team will probably run several of those themselves, or be a prime architect and significant user - but in some cases they may only be a user of the tool, in which case they do need to make sure to be able to give feedback and be heard when doing so. Because of the growing number of possible tools, their 'orchestration' plays a more and more important role. It is of primary interest to any CSIRT to be decisively involved in this area. If a CSIRT deal with some specific types of incidents, it is especially important to create a tailored toolset to suit those specific resolution needs. Bear in mind that this toolset does include software, but can also included dedicated hardware - and in some cases this will go as far as the creation of e.g. an incident resolution lab, e.g. for malware analysis or computer forensics. Examples of resolution tools: again MISP and IntelMQ, your incident tracking system, forensics kits. Does your team have a well-defined incident resolution toolset?

P - Processes

With **Processes** we refer to logically sequenced sets of actions which are carried out by humans (Human area) or automated tools (Tools area) in order to achieve a specific result (defined in the Organisation area). All processes can be characterised by a number of attributes. By applying such attributes we can also determine how successful a particular process is (in getting the job done) or how successful a particular organisation is in providing a service (as in getting this process right all the time). In mature organisations processes are documented, measurable and repeatable. To be able to grow and improve the effectiveness of an organisation it is also important to build processes that are

adaptable. Here, we specifically talk about those processes that support the management of incidents and any other services the CSIRT offers - and we adopt the term 'processes' in the broadest meaning of the word, so that in this Processes area you will also find processes that might sometimes be labeled 'policy' or otherwise.

P-1 Escalation to Governance Level

Description: Process of escalation to upper management for CSIRTs who are a part of the same host organisation as their constituency. For external constituencies: escalation to governance levels of constituents.

Each team must be able to escalate critical incidents to the appropriate management levels, including the highest level of governance (e.g. board of directors, minister) in case of potential crises or incidents that are at least a significant threat to the reputation of the organisation. In case the team is responsible for an external constituency, it also needs to be able to escalate to the appropriate management level of all constituents; the latter is not only required when the team's normal point of contact does not (timely) react, but also such an escalation may be warranted in case of a significant incident or new threat. Such escalations triggered by security incidents or other events should be defined in accordance with the team's Incident Classification (see O-8), which allows logically basing the escalation on e.g. impact and priority. It is critical that the means to escalate must be available at all times - even though the feedback or reaction will not always be as immediate, as this is defined by higher governance levels in the own organisation, or in constituents' organisations. Can your team escalate in the way meant here?

P-2 Escalation to Press Function

Description: Process of escalation to the CSIRT's host organisation's press office.

Handling the press and public media is required. In case most or all CSIRT members have been tasked to not talk with the press themselves, press requests in regard security incidents must still be handled effectively, wherever they come in. Therefore, The team must be able to reach out to appropriate spokes persons who normally handle press inquiries. To avoid miscommunication and delays that might impact the organisation's reputation, the team needs to be able to reach such press contacts directly and also outside business hours, in order to give them the necessary situational awareness. It is advisable that the team itself designates a limited amount of team members to also be able to talk with the press, e.g. together with an official spokes person - as such designated team members will be able to give more insight into the technical aspects of a given situation; when such a choice is made it's advisable to give such team members a suitable training. Can your team escalate in the way meant here?

P-3 Escalation to Legal Function

Description: Process of escalation to the CSIRT's host organisation's legal office.

Handling legal issues including requests from law enforcement is required. Such requests to the organisation must be handled very effectively in order to avoid that evidence is destroyed or no longer available, e.g. as a result of automated processes removing data routinely - but also, because handling such issues wrongly could lead to reputation damage

and financial losses. The team must therefore be able to reach out directly and also outside business hours, to legal experts in their organisation (e.g. lawyers) to inform them about relevant issues, including but not limited to incoming law enforcement requests or orders. The legal experts can then either handle these issues themselves directly, or in consultation with the team. Can your team escalate in the way meant here?

P-4 Incident Prevention Process

Description: Describes how the CSIRT prevents incidents, including the use of the related toolset. Also, this includes the adoption of pro-active services like the issuing of threat/vulnerability/patch advisories.
Clarification: If not applicable as for a purely co-ordinating CSIRT, choose N/A and the parameter will be omitted from 'scoring'.

From a risk management perspective, incidents must be avoided, therefore the CSIRT should support appropriate prevention processes internally - or in case of an external constituency - for its constituents. Examples of processes that prevent incidents from happening are: the creation and dissemination of advisories about new security vulnerabilities; port scan activities; the spreading of threat intel; the sharing of lessons learnt from the analysis of incidents. Usually, tools are used to support these processes (see T-8), and then how to do that will be part of the process. Does your team have a process for incident prevention?

P-5 Incident Detection Process

Description: Describes how the CSIRT detects incidents, including the use of the related toolset.

Without detecting incidents no CSIRT is able to respond to those. Depending on what type of CSIRT we consider, some operate their own detection capabilities (IDS, firewall logs, honeypots, ...). Others are depending on constituents to receive incident reports, or utilise a SOC to receive potential incidents that need to be analysed - a mixed approach is also possible. How to do that is described in the detection process(es).Triage, the process of judging incoming incident reports and assigning them for further handling, is part of incident detection. Usually, tools are used to support these processes (see T-8), and then how to do that will be part of the process. Note that frequently P-5 and P-6 (P-6 follows next and is about incident resolution) are combined in one process, often called the incident management (or handling) process, which is valid as long as both detection and resolution are done justice. Does your team have a process for incident detection? (If you have a combined process for P-5 and P-6, choose the same level for both)

P-6 Incident Resolution Process

Description: Describes how the CSIRT resolves incidents, including the use of the related toolset.

Any CSIRT that manages incidents needs to develop at least a generic process about how to resolve, handle, mitigate incidents. Because it is generic, each input is processed by the very same process in more or less the same way, although most certainly the results will vary. Instead of focusing on the specifics of an incident (e.g. a malware APT is very different from a DDoS attack), this process focuses on the overall step-by-step approach after the detection process (see P-5). The main steps in the process are: analysis, response

actions leading to mitigation, closing and lessons learnt. Following this generic process ensures that all incidents are handled according to the established practice, including the use of the related toolset (see T-10) - this could for example include the logging of all communication with constituents, or the analysis of specific logs, etcetera. Does your team have a process for incident resolution? (If you have a combined process for P-5 and P-6, choose the same level for both)

P-7 Specific Incident Processes

Description: Describes how the CSIRT handles specific incident categories, like phishing, DDoS or copyright issues.
Clarification: This may be part of P-6.

It is very important to have a common process to handle all incidents that are managed by a CSIRT - this is P-6. But such a generic process ensures the overall workflow and can not be tailored for specific types of incidents, and thus will more than likely miss out on some relevant technical aspects. As already stated for P-6, an incident caused by a new malware APT is very different from a DDoS attack blocking the Internet for an important client. Not only are the priorities different, but also the technical response. Therefore it is recommend for mature CSIRTs to identify those incident types that are causing most of the work - and then to write specific incident processes for those. This will allow to leave out some steps or activities, while describing others in more detail or adding new ones (could be sub-steps of the generic process). Additionally, specific incident processes can be written not just for very common incident types, but also for mission critical incidents (high impact, high priority), or for incidents that require a response requiring expertise not commonly present inside the CSIRT itself, like legal expertise. Note that P-7 may be already part of P-6, if the incident resolution process supports sub-processes to deal with some specific incident types or supports various paths for some specific incident types - this is of course perfectly valid. Has your team described specific incident processes, beyond the generic incident resolution process?

P-8 Audit & Feedback Process

Description: Describes what the process is for auditing/assessing the CSIRT and the subsequent feedback to the team. The audit/assessment process can have an internal team self-assessment part, as well as independent auditing. Those elements considered not up-to-standard by the CSIRT and their management are considered for future improvement.
Clarification: With independent auditing is meant any type of auditing not done by the team itself, but rather one that takes place on the authority of higher management layers. This kind of audit can take many shapes: it can still be internal, e.g. by or on behalf of the CISO, or by an audit department. Or it can be external, by means of a subcontractor, or as part of an audit/assessment scheme inside a community of CSIRTs.

All CSIRTs need quality assurance of all critical and sensitive aspects of their operation. While various means exist to help ensure the quality levels (e.g. self-assessment, walk-throughs, peer reviews, internal as well as external audits), the level of scrutiny must be defined, scoped and maintained. Also it needs to be ensured that there is not just 'audit' but also a subsequent feedback to the team, to enable learning and improvement. We call this the audit & feedback process. This process needs to ensure that the appropriate quality levels are met, and that problems are recognised as soon as possible. The resulting

information flow needs to benefit not only the team itself, but also the relevant management layers above the CSIRT. This is especially important for those topics covered by SIM3 Parameters where the team aims to score level 4 - for those, a regular, active form of checking by the higher management (above the CSIRT manager) is required - and it must be documented that they are audited that way and that feedback is given to the team. This involvement of the higher management is a crucial mechanism, as some quality aspects cannot be ensured by the CSIRT itself, not even if controlled by the CSIRT manager or team lead. Unbiased, neutral feedback is mandatory as not to focus on mistakes or errors, but instead to focus on improvement and progress, with the mission of the organisation/constituency in mind. Has such an audit & feedback process been defined for your CSIRT?

P-9 Emergency Reachability Process

Description: Describes how to reach the CSIRT in cases of emergency.
Clarification: Often only available to other teams, partners or specific constituents.

Each CSIRT supports a number of communication mechanisms that can be used to send information or incident reports to. Depending on the constituents need, or the mandate of the CSIRT such means are made publicly known, or are only available for constituents or peer CSIRTs (see P-17). In most cases, CSIRTs service windows coincide with standard business hours. Some CSIRTs are on call outside such times, in accordance with their own service levels. However, crisis/emergency situations can and will occur, and may well require the reachability of the CSIRT even outside the normal service windows. To allow constituents or peer teams to contact the CSIRT in such special cases, there needs to be an emergency reachability process that describes telephone numbers, e-mail addresses and possibly also special keywords reserved for such true emergencies. The process should sanction misuse as reacting outside the normal service windows is usually expensive. On the other hand - given how important it potentially is - the process must be executed from time to time to train all parties involved. Does your CSIRT have such an emergency reachability process?

P-10 Best Practice Internet Presence

Description: This process describes (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) the social media presence.
Clarification: The process needs to take into account, for the three areas mentioned: (1) tracking by the CSIRT of at least the standard e-mail addresses cert@... and security@... - and strongly recommended to take the RFC2142 standard into account and ensure that the relevant mailbox names (postmaster and webmaster deserve special attention) are tracked. And also, that whoever track those mailbox names, know about the CSIRT and how to pass on information to them. (2) a web policy that ensures that all relevant information about the CSIRT is up-to-date and available for the constituency, and a necessary subset including RFC2350 (see O-5) for the world. Additionally it is recommended to consider implementing a slash-security page (example: www.org.tld/security), which can offer a wider range of security related information in regard your (host) organisation, but your CSIRT's info should also be present there. (3) A policy for what social media the team tracks and uses, and how they are to be used. Examples are Twitter, LinkedIN and Facebook.

Minimum Requirement: The process must at least ensure that, for the 3 areas: (1) the mail addresses cert@... and security@... must be tracked by the team; (2) some form of web presence for the CSIRT must exist, at least internally; (3) a policy must be present on if and how to deal with social media.

Good communication is at the heart of the work and success of any CSIRT and being able to reach out over the Internet, and be easily reachable are both essential. Beside having available various communication tools (see T-5, T-6 and T-7), all CSIRTs need a process that specifies which Internet media are used in what way, in order to monitor for incoming requests, share information, etcetera, in order to successfully deliver their various services, and fulfil their mandate and responsibility. The process needs to take into account, for the 3 areas mentioned: (1) tracking by the CSIRT of at least the standard e-mail addresses cert@... and security@... - and strongly recommended to take the RFC2142 standard into account and ensure that the relevant mailbox names (postmaster and webmaster deserve special attention) are tracked. And also, that whoever track those mailbox names, know about the CSIRT and how to pass on information to them. (2) a web policy that ensures that all relevant information about the CSIRT is up-to-date and available for the constituency, and a necessary subset including RFC2350 (see O-5) for the world. Additionally it is recommended to consider implementing a slash-security page (example: www.org.tld/security), which can offer a wider range of security related information in regard your (host) organisation, but your CSIRT's info should also be present there. (3) A policy for what social media the team tracks and uses, and how they are to be used. Examples are Twitter, LinkedIN and Facebook. Does your CSIRT have a process that shapes its Internet presence according to the above best practices?

P-11 Secure Information Handling Process

Description: Describes how the CSIRT handles confidential incident reports and/or information. Also has bearing on relevant legal requirements, including privacy legislation (example: GDPR). Minimum Requirement: The process must support the use of TLP, the Traffic Light Protocol.

Each CSIRT receives and processes information that was labeled confidential by those sending it in - for instance to avoid that the information falls into the hands of attackers, or becomes available on the Internet publicly before appropriate warnings have been distributed. Therefore CSIRTs, but also e.g. vulnerability researchers, are hesitant to share information unless it can be done securely. Now apart from communication security as offered by TLS or security applications like gpg/pgp, the information must also be protected by the receiving CSIRTs (secure storage, backups, etc.) - and this must be done in compliance with relevant legislation, including privacy laws like GDPR. To communicate the restrictions on further distribution of sent information, the TLP (Traffic Light Protocol: see www.first.org/tlp)) protocol has been developed - and any CSIRT is strongly advised to use and adhere to TLP - as a minimum a team must be able to deal appropriately with TLP labeled information. Other protocols also exist, that could be applied in a CSIRT context - but will usually need to be explained. Does your team have a process on how to handle information securely?

P-12 Information Sources Process

Description: Describes how the CSIRT handles the various information sources available to the CSIRT (as defined in the related tool, if available - see T-2).

For each CSIRT it is mandatory to monitor and evaluate appropriate information sources. In addition to public web pages, this could be social media, mailing lists, security vendors, vulnerability databases or exploit sites, portals like pastebin or new alerts sent by information security providers. Regardless how many and what kind of information sources are monitored, the CSIRT needs to develop a process how to do this consistently with the appropriate scrutiny and quality assurance. It must be avoided that the CSIRT acts on wrong or manipulated input, as this will put the reputation of the team at risk. The process must also describe the life-cycle of sources, from being added to the CSIRT's list of information sources - which is T-2 - until removal for reasons of declining quality (or becoming void). Does your team have such a process, linked to the list of sources (T-2)?

P-13 Outreach Process

Description: Describes how the CSIRT reaches out to their constituency not in regard incidents but in regard PR and awareness raising. This process should allow for a two-way channel: the constituency also needs to be able to provide feedback to the team.
Clarification: Please note that feedback from constituency to team (bottom-up) is different from the feedback mentioned in the P-8 process, which is from higher governance to team (top-down).

As the CSIRT offers service to its constituents, it needs to reach out to all constituents and stakeholders. By doing this, it promotes not only itself, but also the best practices and processes recommended by it. While awareness building might be seen as outreach, it is common to label awareness building as a CSIRT service, as it's part of incident prevention and thus core business. However, it is also essential to make sure that the constituency is actively aware of the CSIRT and the services offered. To 'advertise' the team in this way, is part of the outreach process. Equally important is that this process should allow for a two-way channel: the constituency also needs to be able to provide 'bottom-up' feedback to the team (not to be confused with the P-8 feedback which is 'top-down'). The outreach process should include all forms of activities that raise the visibility and reputation of the CSIRT, varying from webpages, via newsletters, webinars, white papers, conferences, etcetera. For any national CSIRT this would include reaching out to the critical infrastructure sectors and ISACs, again in two-way fashion. Does your team have an outreach process?

P-14 Governance Reporting Process

Description: Describes how the CSIRT reports to their higher governance levels. This kind of reporting normally includes statistics and graphics.
Clarification: If the CSIRT is situated inside a host organisation, this process is about the reports sent to the management of the host organisation, and/or to the CISO, CSO or CIO, i.e. internally. In case of a national team, it will be about reporting to the responsible Minister, and possibly to parliament.

By managing incidents for their constituency, the CSIRT gains critical insights otherwise not available to stakeholders, policy makers and even information security or data protection officers. As part of situational awareness (scope will be different according to the aim and objective of the particular CSIRT) the lessons learnt are important to be communicated and escalated. The governance reporting process needs to provide up-to-date reports and background explanations in order to better prevent and remedy similar incidents/attacks/risks in the future. Statistics and graphics based on the types (see O-8)

and number of incidents, resources spent, funding levels, etc. are all part of the governance reporting process. Providing statistics to constituency or public, is covered by P-15. Does your CSIRT report to higher governance according to a set process?

P-15 Constituency Reporting Process

Description: Describes what the CSIRT reports to their constituency and/or beyond (potentially to the world).
Clarification: This kind of reporting can vary from concise and generic, to more detailed, including statistics and graphics (based on their incident classification, see O-8). Sometimes - especially with national CSIRTs - it takes the form of annual trend reports. It is also valid to explicitly choose to report internally only and not to the constituency: in that case choose N/A and the parameter will be omitted from 'scoring'.

Whereas P-14 is about reporting to higher governance, P-15 is about reporting to the constituency - or even to the world at large (like e.g. several national teams do, in annual trend reports). Statistics and graphics may be included in such reporting - and just like for P-14, it is useful to base such more detailed reporting on the typology used for incidents (see O-8) - and to do that using a (semi-)automatic export from internal typology and numbers to the required external format(s). Note that there may be other reporting schemes, for example mandatory reporting according to national laws based on different premises. Does your team offer this kind of statistics to constituency or public, and is there a process for doing so?

P-16 Meeting Process

Description: Defines the internal meeting process of the CSIRT.
Clarification: This can include online and hybrid meetings.

The CSIRT's internal communication and effectiveness can be greatly improved by regular meetings, usually weekly or even daily. Various needs exist, and also different organisation set-ups (including having people in more than one location), therefore no fixed schedule is imposed. But all teams need to consider the appropriate number of meetings, the scope of such meetings and their modus operandi: live, online or hybrid. As a minimum the meeting process needs to ensure that action points as well as lessons learnt are captured and distributed to all involved. As grounds can easily be found to cancel team meetings, the process must ensure that there is a mandatory minimum number of meetings that take place and are attended by the required mix of roles/persons. Allowing for hybrid team meetings make this goal easier to achieve. Does your team have a well defined meeting process?

P-17 Peer Colloboration Process

Description: Describes how the CSIRT works together with peer CSIRTs and/or with their "upstream" CSIRT - and also with peers among other types of security teams like SOCs, PSIRTs, ISACs, etcetera.
Clarification: A peer team is a security team with which a special kind of relationship exists, based on a shared membership of some community or cooperation, or on MoU type agreements.
Minimum Requirement: The process must define what 'peers' exist, and ensure that with those peers a two-way trusted communication is established.

It is important to be a member or part of relevant communities in order to foster trust relationships with other teams, in order to gain better information more timely, and to improve communication, both in terms of speed and of quality. Also, several teams will be part of a more hierarchically structured context - for example a CSIRT in a commercial organisation may need to report into a coordinating CSIRT on the corporate level - or lower level government teams may need to report into a national CSIRT. In all case such 'peer' relationships need to be defined and appropriate processes need to be defined on both sides. If there is a hierarchical structure, the consequences of this need to be clearly documented. When the peers are more like 'fellow' teams in a non-hierarchical context (e.g. the membership of FIRST, or of regional CSIRT cooperations), it still needs to be defined how those 'peers' work together and what expectations and processes are in place. Also it must be taken into account that 'peers' can obviously be other CSIRTs, but can also be found among other types of security teams like SOCs, PSIRTs, ISACs, etcetera. Has your team defined what their various 'peers' are, and what the process(es) towards those peers is/are?

Copyright

Open CSIRT Foundation 2016-2023 and onwards; with unlimited right-to-use and re-use for S-CURE bv, PRESECURE Consulting GmbH and Fundacja Bezpieczna Cyberprzestrzen from 2008-2022, providing this copyright statement stays in place.