

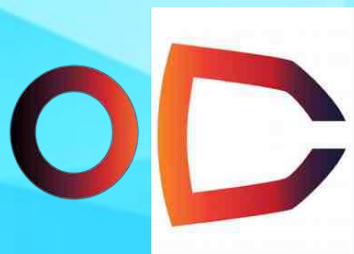


Funded by the European Union



SIM3 Training

OLIVIER CALEFF



**Open CSIRT
Foundation**



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY



Foreign, Commonwealth
& Development Office



Ministry of Foreign Affairs of the
Netherlands

Why would you listen to us ?

How “mature” are the CSIRTs I know ?

Is that just gut feeling ?

What is this “maturity” really ?

How do I assess or measure it ?

Are there common standards of maturity ?

What about audits ?



SIM3... Starting to drill down

44 parameters in 4 categories and in 5 maturity levels

Organisation: 10

Human Aspects: 7

Tools: 10

Processes: 17

0 = not available

1 = implicit

2 = explicit, internal

3 = explicit, formalised by
CSIRT authority

4 = explicit, assessed by governance
levels on a regular basis

CSIRTs – Computer Security Incident Response Teams

Internet "worm" Nov'88

CERT & similar teams started '89 → FIRST European
cooperation since '93 → TF-CSIRT Commercial teams
entered around '95

Govt teams around 2000, later also national teams, military, CIIP, etc

**CSIRT system = worldwide mesh of CSIRT/CERTs at all levels that
works ... fascinatingly well**

Includes NCSCs, ISACs, SOCs etc

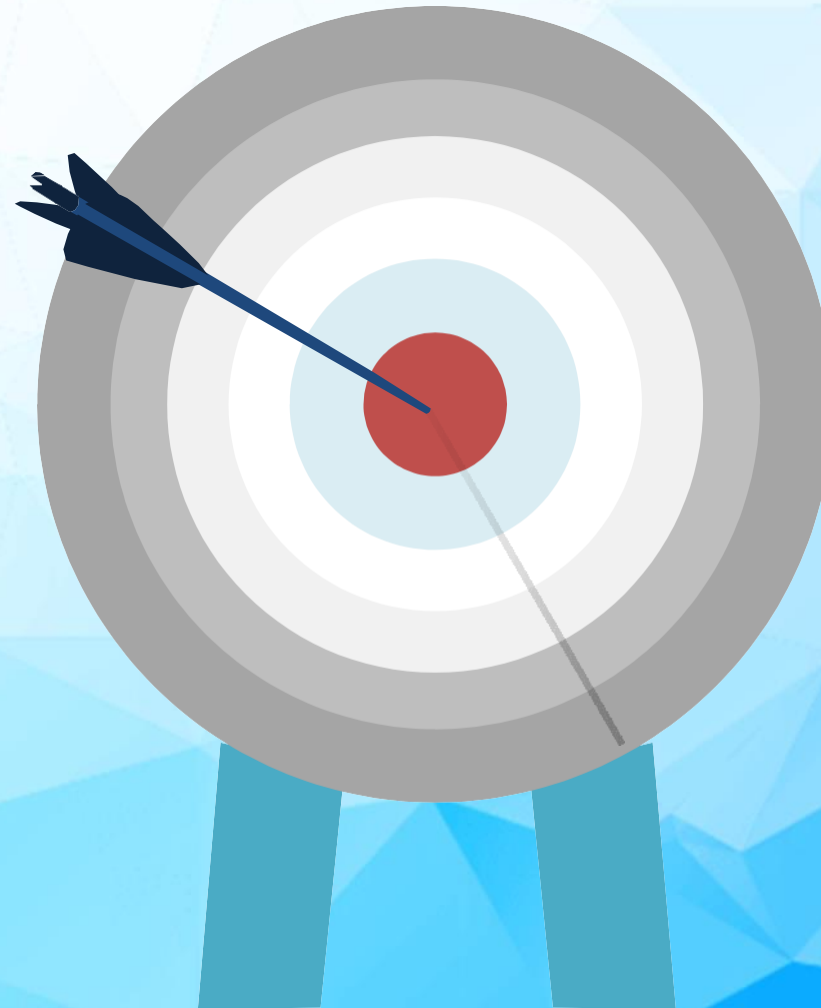


Training Objectives

SIM3 deep dive

How to use SIM3 for self-assessment

Prepare for assessments and audits



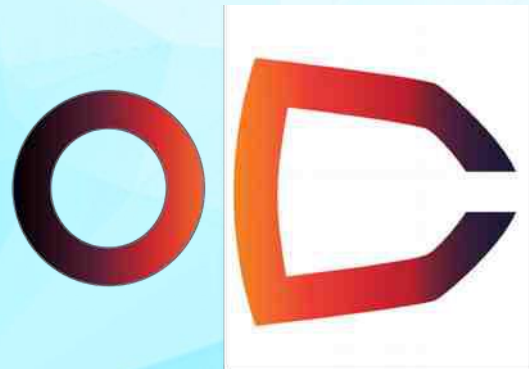
CSIRT Maturity

An indication of how well a team governs, documents, performs and measures their function.

Increasing focus (chronologically)

- CERT/CC e.g. CERT-RMM (Resilience Management Model)
- TF-CSIRT uses SIM3 for Certification of teams since 2010
- ENISA “baseline capabilities” & recent SIM3 based developments
- CyberGreen focuses on cyber security “health” measurements
- CSIRT Maturity Kit by GFCE & NCSC-NL (SIM3 based)
- FIRST is working on CSIRT & PSIRT services
- OCF stewardship of SIM3
- NCA (Nippon CSIRT Association, 250+ members) uses SIM3 for maturity development
- FIRST is working on adopting SIM3 as part of membership process
- GFCE : brand-new development for national CSIRTs

OCF : Open CSIRT Foundation



**Open CSIRT
Foundation**

Foundation (NL law), born on 21 Oct 2016

Goal is to *stimulate the state-of-the-art in Internet security and resilience worldwide, in order to contribute to democracy as well as personal freedom.*

In order to achieve that goal, the Foundation will stimulate and facilitate relevant services, research, trainings, education, standardisation, best practices and any other associated activities.

Governance:

- Board of Directors (chair: Don Stikvoort; secretary: Mirosław Maj; cfo)
- Board of Commissioners: global scope, under construction

Financial: not-for-profit

SIM3 primer (i)

SIM3 = Security Incident Management Maturity Model

- For (self) assessment,
- membership criteria &
- certification purposes

44 parameters in 4 categories

- Organisation : 10 (11 minus 1)
- Human Aspects : 7
- Tools : 10
- Processes : 17

SIM3

primer

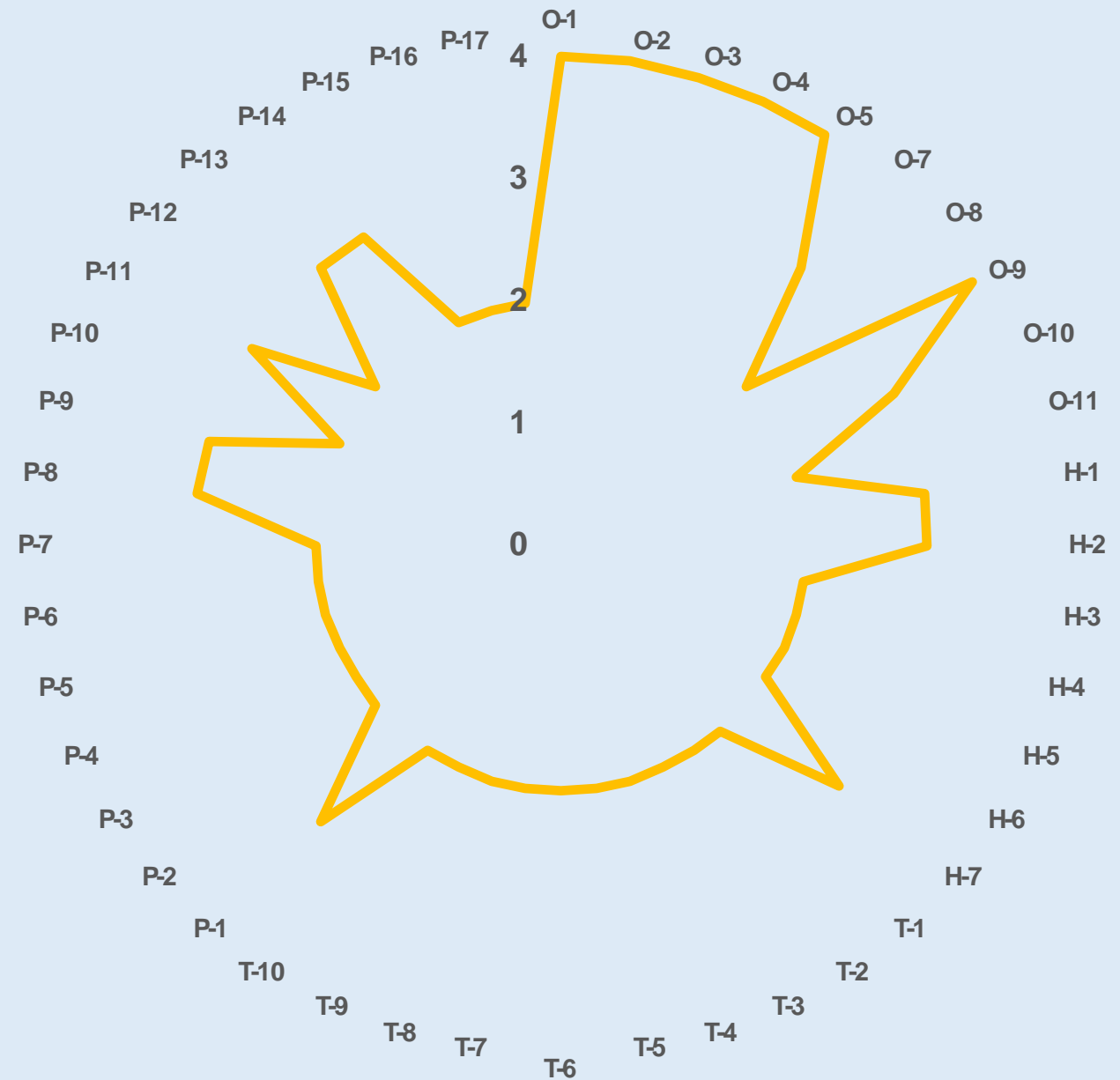
(ii)

Each parameter can score :

- 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 CSIRT head (“rubberstamped” or published)
- 4 = explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis (subject to control process/review)

SIM3 primer (iii)

ASSESSED CSIRT MATURITY EXAMPLE



European approach

TF-CSIRT / Trusted Introducer (initiated 1993, formally founded 2000)

Membership stages :

- LISTED : requires 2 sponsors – since 2001
- ACCREDITED : full membership – since 2001
- CERTIFIED : **optional** certification – since 2010

Certification was introduced to help teams increase maturity level

- Formal process based on SIM3 maturity model
- Minimum values were set for all 44 parameters in 2010 (update when?)
- Re-Certification every 3 years

Status today :

- Around 25 Certified teams



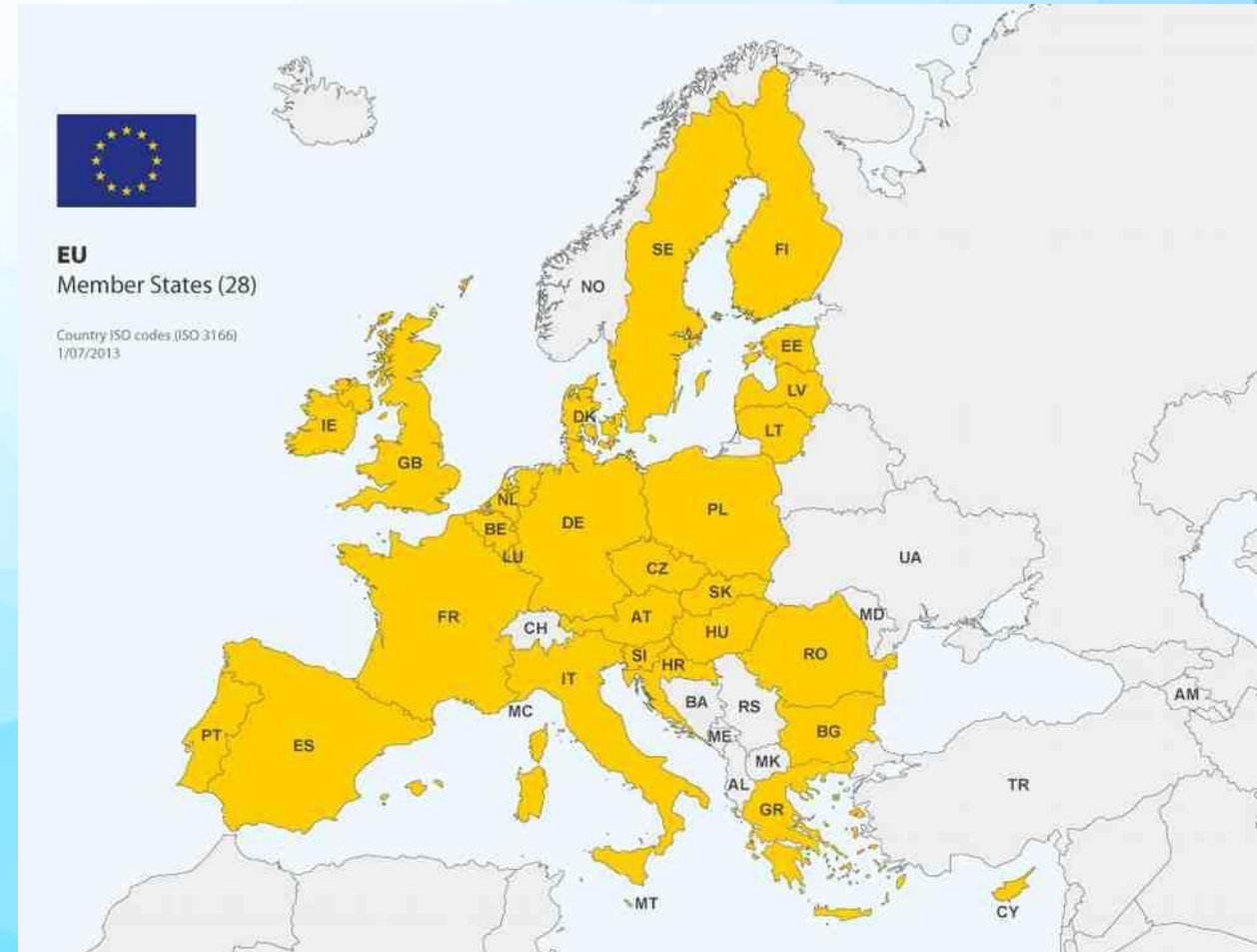
EU NIS Directive

CSIRTs network

- 28+ n/g CSIRTs ; ENISA is caretaker
- Support to increase maturity across the board
- NIS Directive demands higher than existing Certification

Step-by-step approach leading beyond
“Certification” level

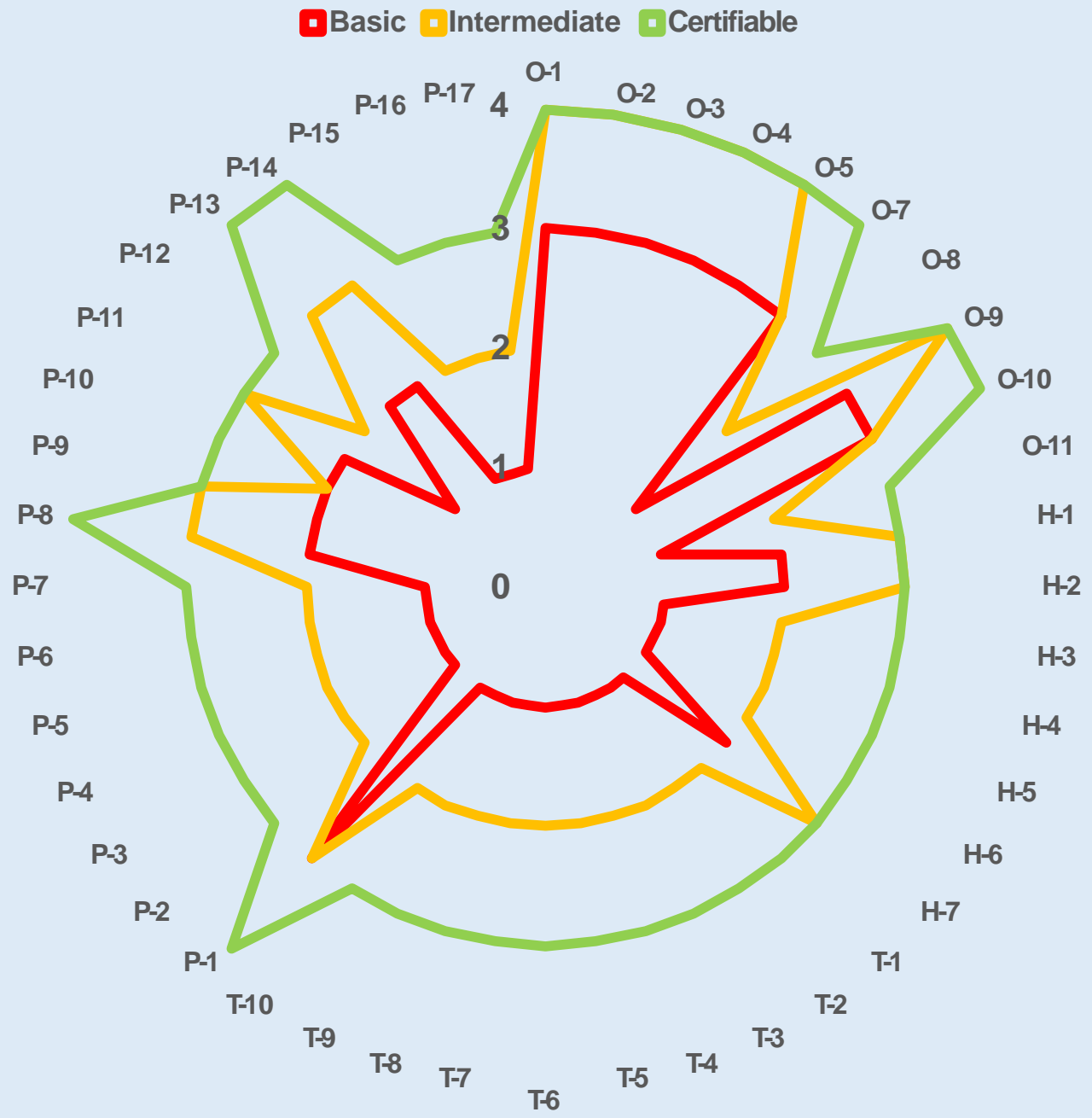
SIM3 based



ENISA approach : increasing maturity in 3 steps



CSIRT MATURITY EVOLUTION IN 3 STEPS



ENISA approach : assessment

- ***Self-assessment***

- Questions and answers for all parameters
- Mapping to the proposed 3 steps Basic
- Intermediate
Advanced

Peer review

Community driven approach :
Peer review

Mutual support

ENISA approach : self-assessment

Questions and answers for all 44 SIM3 parameters

Do-it-yourself

Less objective than the externally assessed TI Certification proces

Very useful for stimulating evolution in a community

Peer review worthwhile addition



O-2

QUESTION

O-2: Does your CSIRT have a clear constituency, that is, the target group for who you do the CSIRT work, your "client base"?

ANSWERS

LEVEL

We never really discussed this.

0

We know our constituency, but it was never written down.

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.

2

We have a written constituency definition approved by our team management.

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.

4

T-9

QUESTION	
T-9: Does your CSIRT have a collection of tools aimed at detecting incidents when they happen or are near to happen?	
ANSWERS	LEVEL
We never really discussed this.	0
We have such tools, but have not listed or documented them.	1
We have such tools, and to record this we wrote something for our own purposes. Our management has not formally approved this.	2
We have such tools, have documented these and this was approved by our team management.	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.	4

ENISA has placed the self-assessment online

<https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey>

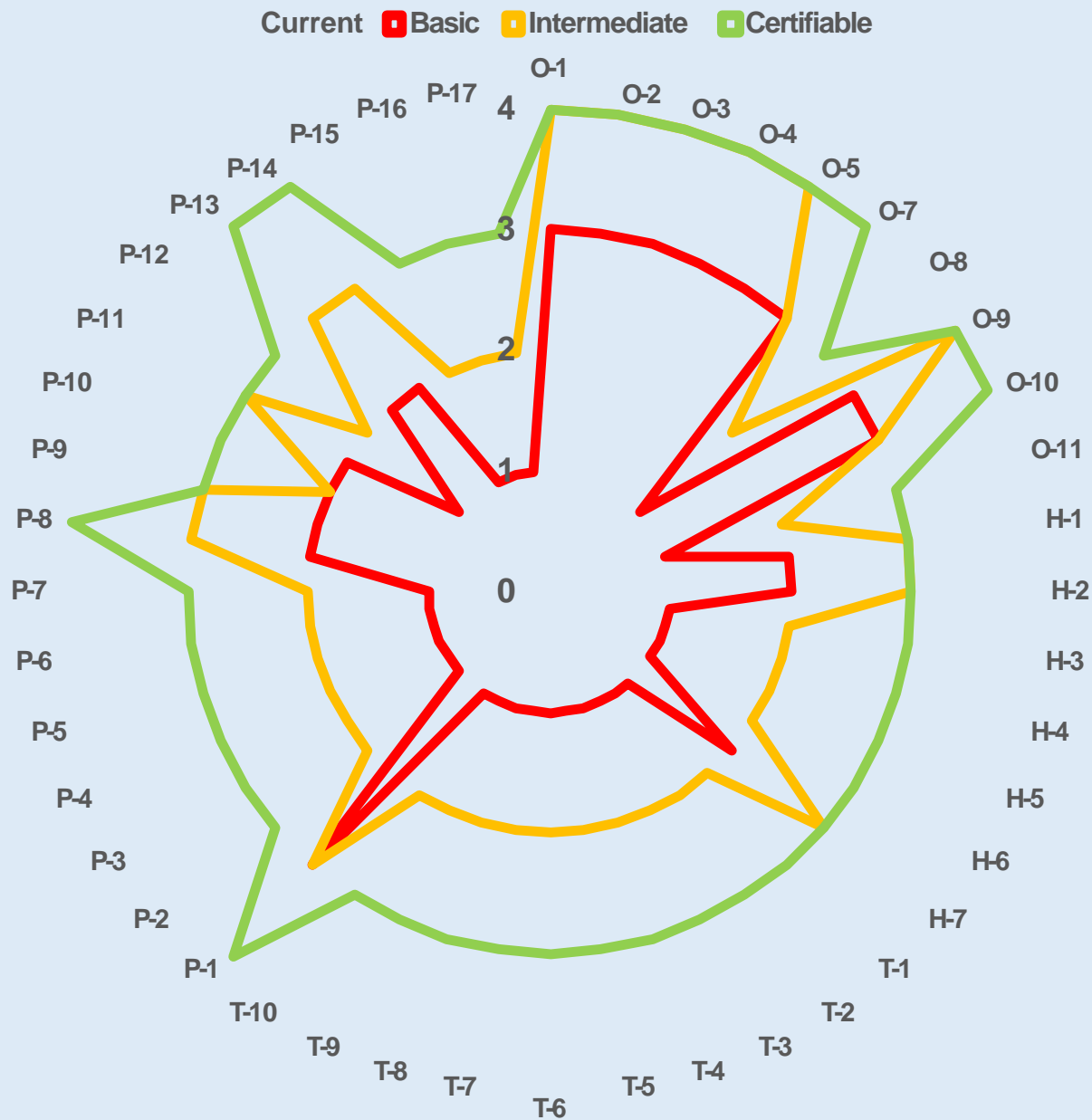
It looks like this for all 44 parameters/questions :

P-8: Audit/Feedback Process

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.

We have a formal written process approved by our team management and by higher management, and higher management is leading in this ⬆

CURRENT CSIRT MATURITY COMPARED TO 3 MATURITY STEPS



Peer review methodology

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 and to whom ?



A step back to SIM3

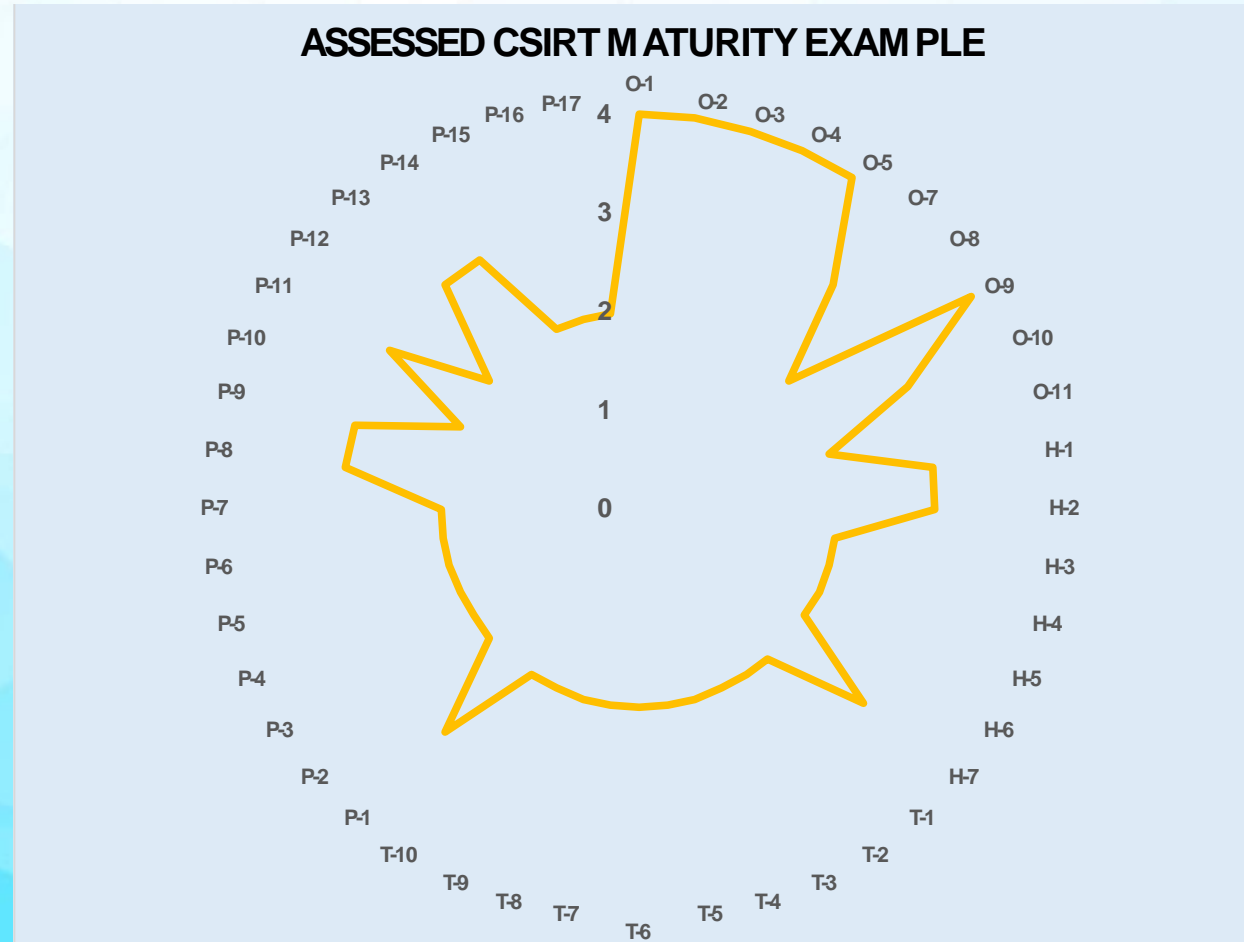
SIM3 used by TF-CSIRT, CSIRTs network, NCA, GFCE, FIRST and others, including consultancy companies

The use of SIM3 v1 is free

OCF has been given this role and fulfills it **not for profit**

- Defined “Certified SIM3 Auditors”
- 13 Certified SIM3 Auditors now

The SIM3 parameters one-by-one



3 basic approaches towards increasing maturity as per SIM3

1. Improve maturity per parameter. For all 44 parameters.
Do fill out rfc2350.
2. Write at least the following documents additional to rfc2350:
 - Organisational Framework, covering most O parameters, plus some H and P;
 - Staff hiring and development policy, covering most H parameters;and handle the rest per parameter.
3. Write a full CSIRT Maturity "handbook" covering all parameters.
Do fill out rfc2350.

The levels in depth (i)

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 CSIRT head (“rubberstamped” or published)


4 = explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis (subject to control process/review)

The levels in depth (ii)

 → 1 : addition of *consideration* - “listen, we are aware of this”

 → 2 : addition of *written description* - “read, this is the way we do it”

 → 3 : addition of *accountability* - “look, this is what we are bound to do”

 → 4 : addition of *control mechanism* – “and this is how we make sure that it happens”

The levels in depth (iii) – evidence, substantiation, proof

1 : n/a

2 : they have to be able to talk about it and make sense

3 : wiki pages (not approved), informal documents

For audits you got to SEE them

3 : documents approved by the team management – can also be on wiki, but beware of maintenance

For audits you got to SEE them

4 : like 3, but you need to substantiate that it is “actively assessed on authority of governance levels above the CSIRT management on a regular basis”

For audits you got to SEE this ; possibly see review/audit reports

Format of the parameter slides

First follow “description” and other tags as per “SIM3 mkXVIIIb, Don Stikvoort, 30 March 2015”. The tag definition from SIM3:

[Parameter Identifier] : [Parameter Name:]

Description:

{ OPTIONAL: Clarification: }

{ OPTIONAL: Minimum Requirement: }

{ OPTIONAL: Accreditation Requirement: }

{ OPTIONAL: Certification Requirement: }

Next the Question from the ENISA self-assessment (OCF supported)

P-8 Audit/Feedback Process

- Description: Describes how the CSIRT assesses their set-up and operations by self-assessment, external or internal assessment and a subsequent feedback mechanism. Those elements considered not up-to-standard by the CSIRT and their management are considered for future improvement.
- 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.

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 CSIRT's mission and parameters O-1 to O-9.

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.

O-5 Service Description

Description: Describes what the CSIRT service is and how to reach it.

Minimum requirement: Contains the CSIRT contact information, service windows, concise description of the CSIRT services offered and the CSIRT's policy on information handling and disclosure.

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.

O-1 Mandate

Description: The CSIRT's assignment as derived from upper management.

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).

O-2

Constit

uency
Description: Who the CSIRT functions are aimed at – the “clients” of the CSIRT.

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).

O-3 Authority

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

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.

O-4 Responsibility

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

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

O-5 Service Description

Description: Describes what the CSIRT service is and how to reach it.

Minimum requirement: Contains the CSIRT contact information, service windows, concise description of the CSIRT services offered and the CSIRT's policy on information handling and disclosure.

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.

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.

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.

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.

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).

O-9 Integration in Existing 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).

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.

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 CSIRT's mission and parameters O-1 to O-9.

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.

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.

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.

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. 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.

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.

H-2 Personal Resilience

Description: How CSIRT staffing is ensured during illness, holidays, people leaving, etc.

Minimum requirement: three (part-time or full-time) CSIRT members.

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.

H-3 Skillset

Description

Description: Describes the skills needed on the CSIRT job(s).

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.

H-4 Internal Training

Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones.

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.

H-5 External Technical Training

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

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.

H-6 (External) Communication Training

Description: Program to allow staff to get (human) communication/presentation training externally.

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.

H-7 External Networking

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

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.

T-1 IT Resources List

Description: Describes the hardware, software, etc. commonly used in the constituency, so that the CSIRT can provide targeted advice.

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.

T-2 Information Sources List

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

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.

T-3 Consolidated E-mail System

Description: When all CSIRT mail is (at least) kept in one repository open to all CSIRT members, we speak of a consolidated e-mail system.

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

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: RTIR, AIRT, OTRS, trouble ticket systems in general.

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.

T-5 Resilient Phone

Description: The phone 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: Mobile phones are the easiest fallback mechanism for when a team's landlines are out of order.

Minimum requirement: Fallback mechanism for the case of phone system outages

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.

T-6 Resilient E-mail

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

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?

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.

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?

T-8 Incident Prevention Toolset

Description: A collection of tools aimed at preventing incidents from happening in the constituency. The ' 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 -1 as Level and will be omitted from "scoring".

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.

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, Quarantinenets, netflow analysis.

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).

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.

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.).

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.

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.

P-2 Escalation to Press Function

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

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?

P-3 Escalation to Legal Function

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

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?

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.

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.

P-5 Incident Detection Process

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

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.

P-6 Incident Resolution Process

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

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.

P-7 Specific Incident Processes

Description: Describes how the CSIRT handles specific incident categories, like phishing or copyright issues.

Clarification: may be part of P-6.

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.

P-8 Audit/Feedback Process

- Description: Describes how the CSIRT assesses their set-up and operations by self-assessment, external or internal assessment and a subsequent feedback mechanism. Those elements considered not up-to-standard by the CSIRT and their management are considered for future improvement.
- 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.

P-9 Emergency Reachability Process

Description: Describes how to reach the CSIRT in cases of emergency.

Clarification: Often only open to fellow teams.

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.

P-10 Best Practice Internet Presence (i)

Description: 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 – and (2) the web 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](http://www.org.tld/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.

P-10 Best Practice Internet Presence (ii)

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.

P-11 Secure Handling Process Information

Description: Describes how the CSIRT handles confidential incident reports and/or information. Also has bearing on local legal requirements.

Clarification: it is advised that this process explicitly supports the use of ISTLP, the Information Sharing Traffic Light Protocol⁴. (In the next version of this document this advise will most likely become a requirement.)

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.

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).

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)?

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.

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.

P-14 Reporting Process

Description: Describes how the CSIRT reports to the management and/or the CISO of their host organisation, i.e. internally.

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?

P-15 Statistics Process

Description: Describes what incident statistics, based on their incident classification (see O-8), the CSIRT discloses to their constituency and/or beyond.

Clarification: If not applicable as in case of an explicit choice only to report internally, choose -1 as Level and will be omitted from “scoring”.

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.

P-16

Meeting

Process Description: Defines the internal meeting process of the CSIRT.

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

P-17 Peer-to-Peer Process

Description: Describes how the CSIRT works together with peer CSIRTs and/or with their “upstream” CSIRT.

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.



Funded by the European Union



SIM3 Training

OLIVIER CALEFF



**Open CSIRT
Foundation**



NI·CO



REPUBLIC OF ESTONIA
INFORMATION SYSTEMS AUTHORITY



Foreign, Commonwealth
& Development Office



Ministry of Foreign Affairs of the
Netherlands