SIM3 – the maturity model to build and strengthen incident management capabilities

Maciej Pyznar

comCERT

Whois

1. Director of the Services Department, ComCERT SA
    - SOC Team
    - CERT Team
    - Cybersecurity Processes Team
2. Head of Critical Infrastructure Protection Unit, Government Centre for Security
3. LA22301
4. SIM3 certified auditor

Short agenda

1. What SIM3 is

2. How SIM3 can be used

SIM3?

SIM3 : Security Incident Management Maturity Model

SIM3

The maturity model is built on three basic elements:

- Maturity Parameters
- Maturity Quadrants
- Maturity Levels

The parameters are the quantities that are measured in regard to the maturity. SIM3 model includes 44 parameters.
Each parameter belongs to one of four quadrants describing their scope and context:

- O – Organization: 10 → 0-1 to O-11
- H – Human: 7 → P-1 to P-7
- T – Tools: 10 → T-1 to T-10
- P – Processes: 17 → T-1 to T-17

SIM3 parameter measurement scale

Scale	Status	Indicators
0	Not available / undefined / unaware	none (“We never really discussed this”)
1	Implicit	Known/considered but not written down, ‘between the ears’, ‘tribal knowledge’ (“We know about it, care about it, but it was never written down”)
2	Explicit, internal	Written down but not formally adopted or reviewed (“We have a draft… never formalized”, “Management didn’t formally approved it”)
3	Explicit, formalised on authority of CSIRT head	Approved or published (“Here is the document, with the management validation”)
4	Explicit, actively assessed on authority of governance levels above the CSIRT management on a regular basis	Subject to a control process and/or review (“Here is the review process, and the changes, with timestamped log of all”)

SIM3 “O” parameters

- O-1 – Mandate
- O-2 – Constituency
- O-3 – Authority
- O-4 – Responsibility
- O-5 – Service Description
- O-7 – Service Level Description
- O-8 – Incident Classification
- O-9 – Participation in Existing CSIRT Frameworks
- O-10 – Organisational Framework
- O-11 – Security Policy

O-1 & O-2

- **O-1 – Mandate**
  - *Description: The CSIRT’s assignment as derived from upper management*
  - Does your CSIRT have a mandate?
- **O-2 – Constituency**
  - *Description: Who the CSIRT functions are aimed at – the “clients” of the CSIRT*
  - Does your CSIRT have a clear constituency? What is the target group your team works for/delivers services to?

SIM3 “H” parameters

- H-1 – Code of Conduct/Practice/Ethics
- H-2 – Personal Resilience
- H-3 – Skillset Description
- H-4 – Internal Training
- H-5 – (External) Technical Training
- H-6 – (External) Communication Training
- H-7 – External Networking

H-3 & H-4

- **<u>H-3 – Skillset Description</u>**
  - *Description: Describes the skills needed on the CSIRT job(s)*
  - Does your CSIRT have a description of the skills needed on the CSIRT position(s) that you have inside your team?
- **<u>H-4 – Internal Training</u>**
  - *Description: Internal training (of any kind) available to train new members and to improve the skills of existing ones*
  - 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?

SIM3 “T” parameters

- T-1 – IT Resources List
- T-2 – Information Sources List
- T-3 – Consolidated E-mail System
- T-4 – Incident Tracking System
- T-5 – Resilient Phone
- T-6 – Resilient E-mail
- T-7 – Resilient Internet Access
- T-8 – Incident Prevention Toolset
- T-9 – Incident Detection Toolset
- T-10 – Incident Resolution Toolset

T-1 & T-2

- **T-1 – IT Resources List**
  - *Description: Describes the hardware, software, etc. commonly used in the constituency, so that the CSIRT can provide targeted advice*
  - 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?
- **T-2 – Information Sources List**
  - *Description: Where does the CSIRT get their vulnerability/threat/scanning information from?*
  - Does your CSIRT maintain a list of sources (info feeds, websites, newspapers, tweets, etc.) where they get their vulnerability/trend/scanning information from?

SIM3 “P” parameters

- P-1 – Escalation to Governance Level
- P-2 – Escalation to Press Function
- P-3 – Escalation to Legal Function
- P-4 – Incident Prevention Process
- P-5 – Incident Detection Process
- P-6 – Incident Resolution Process
- P-7 – Specific Incident Processes
- P-8 – Audit/Feedback Process
- P-9 – Emergency Reachability Process
- P-10 – Best Practice Internet Presence
- P-11 – Secure Information Handling Process
- P-12 – Information Sources Process
- P-13 – Outreach Process
- P-14 – Reporting Process
- P-15 – Statistics Process
- P-16 – Meeting Process
- P-17 – Peer-to-Peer Process

P-5 & P-6

- **<u>P-5 – Incident Detection Process</u>**
  - *Description: Describes how the CSIRT detects incidents, including the use of the related toolset*
  - Does your CSIRT have a process describing the activities aimed at detecting incidents, including the use of the related toolset?
- **<u>P-6 – Incident Resolution Process</u>**
  - *Description: Describes how the CSIRT resolves incidents, including the use of the related toolset*
  - Does your CSIRT have a process describing the activities aimed at resolving incidents, including the use of the related toolset?

SIM3 in the world

- TF-CSIRT / Trusted Introducer – the European CSIRT cooperation, has used SIM3 since 2010 for an optional Certification of their Accredited members.
  - ➢ Certification was introduced to help teams increase maturity level
  - ➢ Formal process based on SIM3 maturity model (audit)
  - ➢ Minimum values were set for all 44 parameters
  - ➢ Status today: 40 Certified teams
- ENISA – adopted SIM3 as the starting point for their staged maturity approach for the national CSIRTs in the European Union.
  - ➢ EU NIS Directive → CSIRTs network
  - ➢ "baseline capabilities" → CSIRTs Network members
  - ➢ 3 levels : 1 – Basic, 2 – Intermediate, 3 – Advanced
- The Nippon CSIRT Association (NCA), the Japanese cooperation society for over 300 CSIRTs, uses SIM3 for improving the maturity of their members
- FIRST is working on taking up SIM3 as part of their membership framework

SIM3 related materials

- OpenCSIRT Web site
  - https://opencsirt.org/
- SIM3 version mkXVIIIb (September 2018)
  - https://opencsirt.org/maturity/sim3/
  - https://ocfweb.files.wordpress.com/2018/10/sim3-mkxviiib.pdf

comCERT

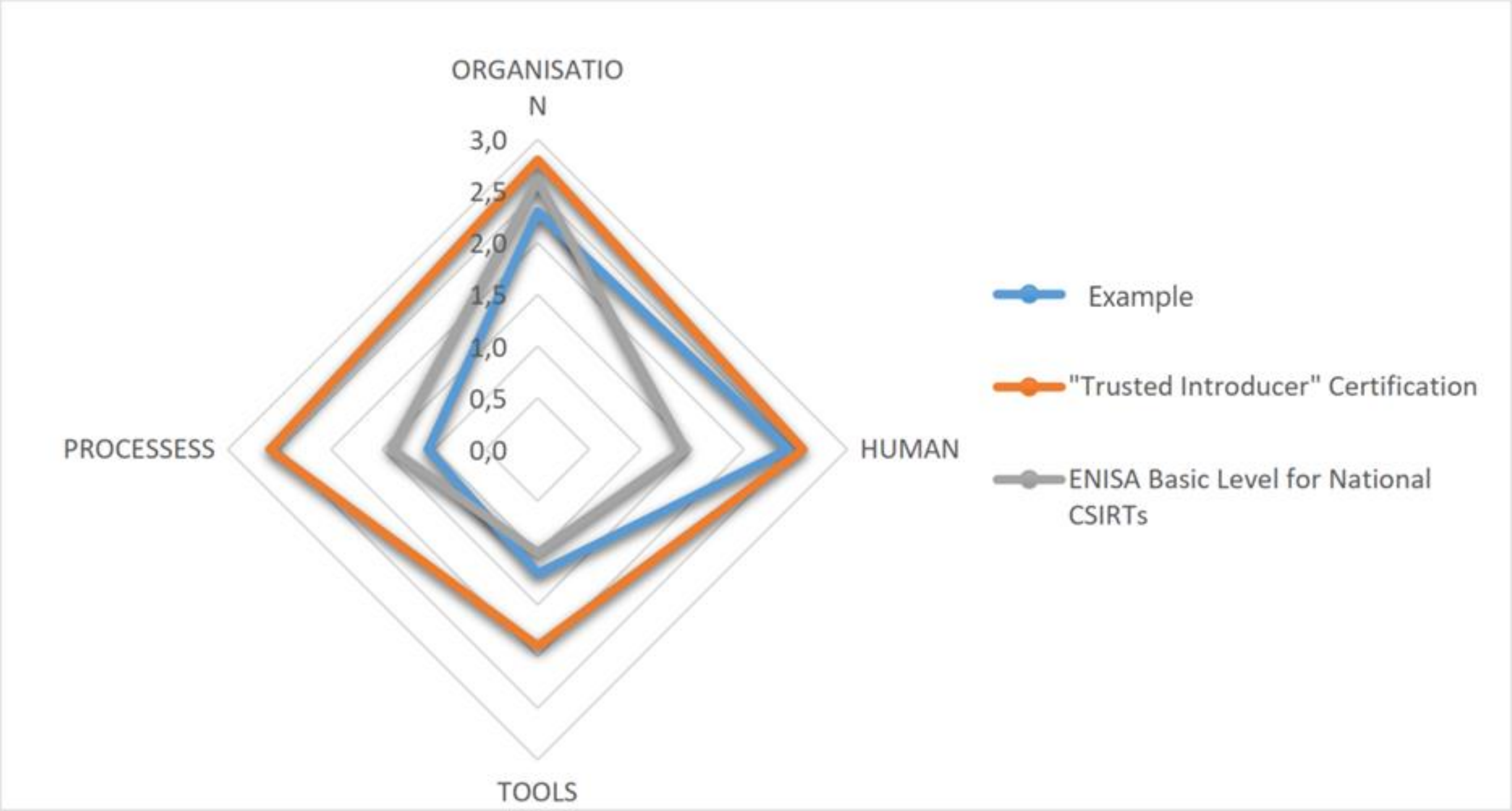
Usage of the SIM3

1. Meeting formal requirements wher SIM3 is required:
   - Membership criteria
   - Certification purposes
2. SOC/CERT development process
   - Self assessment
   - Initial assassment (at the beginning of project – decalration)
   - Actual assessment (with analysis of documentation and verification)
   - Progress assessment (monitoring of changes)

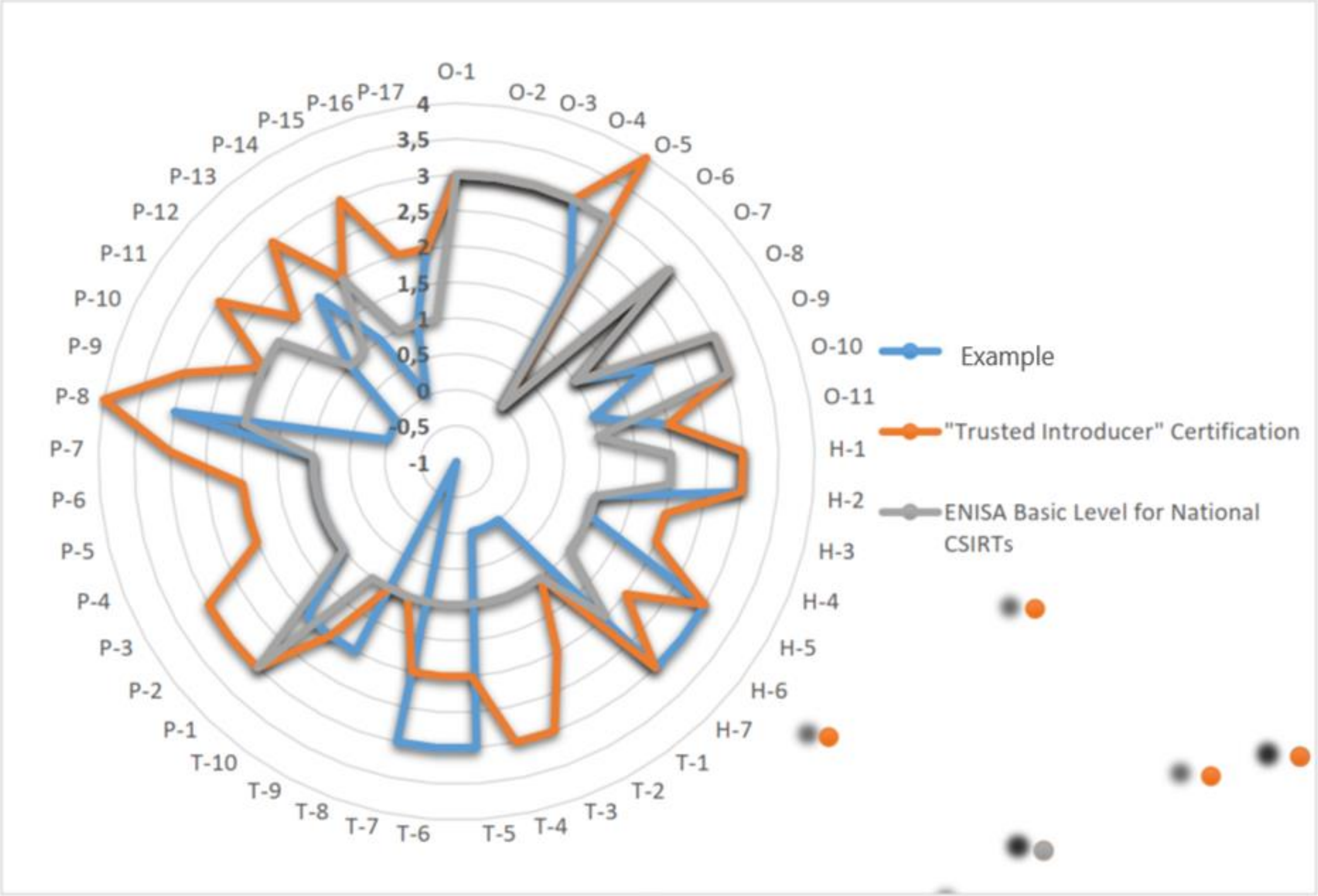
SOC/CERT development process

Parameter	Description	Level	Findings
<Quadrant ID> - <Parameter ID>	<PARAMETER NAME> Description: <freetext>	#	<Findings from the Assessement>

Graphic representation



Graphic representation



comCERT

Recommendations

Parameter	Recommendation (example)	Priority (1,2,3)
O-2	Define precisely the organization CERT area of operation (constituency), both in a technical way (IP, AS, DNS) and by identifying the characteristics of the resources used. It is absolutely necessary to have access to the constituency resources register, including OT devices (the CERT have to know whether the potential event relates to its constituency)	1
O-3	Supplement the regulations with CERT permitions, in particular to issuing orders regarding cybersecurity to the constituents	2
O-4	Develop documentation containing: 1) the scope of operation and powers of individual organizational units of the CERT 2) structure and FTEs (specific structure, number and type of positions and organizational units included in the CERT)	2

To make life easier

https://sim3-check.opencsirt.org/#/

Thank you for your attention

comCERT

ComCERT SA

ul. Adama Branickiego 13, 02-972 Warszawa

e-mail: biuro@comcert.pl tel.: +48 22 112 06 83 www: comcert.pl

NIP: 5252524691 **KRS:** 0000406425 **REGON:** 145934931