



Measure and Improve National CIRT Maturity

ITU CyberDrill 2021, 14 October 2021

PRESENTERS: MIROSLAW MAJ & DON STIKVOORT

INFO@OPENCSIRT.ORG

WWW.OPENCIRT.ORG

© 2017-2021 OPEN CSIRT FOUNDATION

Why listen ?



- How “mature” are the CSIRTs I know ?
- Is that just gut feeling ?
- What is this “maturity” really ?
- How do I measure it ?
- Is there a CSIRT maturity standard ?

Whois Don Stikvoort?

FIRST Incident Response Hall of Fame Inductee :




<https://www.first.org/hof/inductees#don-stikvoort>

© 2017-2021 OPEN CSIRT FOUNDATION

Whois

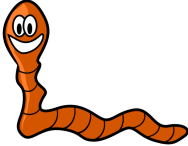

Mirosław Maj ?
 Polish cyber security and CSIRT pioneer
https://pl.wikipedia.org/wiki/Miros%C5%82aw_Maj

Don Stikvoort ?
 FIRST Incident Response Hall of Fame Inductee
<https://www.first.org/hof/inductees#don-stikvoort>

© 2017-2021 OPEN CSIRT FOUNDATION

C(S)IRT system

- Internet "worm" Nov'88
- CERT & similar teams started '89 → FIRST
- Regional cooperation examples

Europe since '93 → TF-CSIRT	Asia since '97 → APCERT, APNIC, ASEAN
Latin America since → OAS & LACNIC	Africa since '11 → AfricaCERT, WACREN et al
- Commercial company teams entered around '95
- Govt teams around 2000, later also national teams, military, CIIP ...
- ITU, GFCE, ...
- Add NCSCs, ISACs, SOCs, ...

CSIRT system = worldwide mesh of CSIRTs at all levels that works fascinatingly well

© 2017-2021 OPEN CSIRT FOUNDATION

What's in a name



- “What’s in a name? That which we call a rose
By any other name would smell as sweet.” Romeo and Juliet, William Shakespeare
- CERT since 1988
- CSIRT sinds 1998
- ITU uses CIRT
- IHT, IHC, SIRT, CDC, ...
- National C(S)IRT = nCSIRT, NCSC
- PSIRT, ISAC, SOC, ...
- CSIMC ;) – ugly, but →

© 2017-2021 OPEN CSIRT FOUNDATION

Incident Management



- CSIRT Handbook (1998-2003)
 - <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305>
 - Proactive → reactive → security quality management services
- ENISA: Good Practice Guide for Incident Management (2010)
 - <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>
 - Introduces Incident Management as a cycle of:
 - {Preparation} <<< the missing link
 - Prevention <<< national teams do this too !
 - Detection <<< includes SOC
 - Resolution <<< the “R” in CERT/CSIRT/CIRT
 - Lessons learnt <<< quality management, feeding back into the 2 Ps above

© 2017-2021 OPEN CSIRT FOUNDATION

What is maturity?



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

Maturity: from *word of mouth* and *ad hoc* practices, towards ...

- a well-cemented organisational set-up
- explicit attention to the *amazing* people working in the team
- properly managed and documented tools
- validated processes
- all reviewed on a regular basis and improved as part of maturity and quality assurance

© 2017-2021 OPEN CSIRT FOUNDATION

SIM3 in a nutshell



Security Incident Management Maturity Model

1 2 3

<https://opencsirt.org/csirt-maturity/sim3-and-references/>

44 parameters in 4 categories and 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

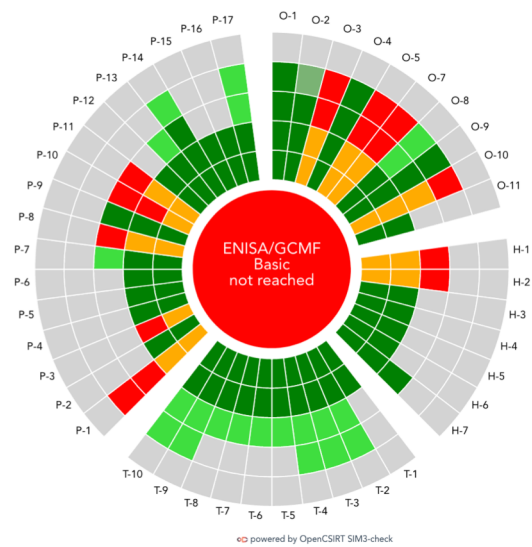
4 = explicit, **regularly** assessed by **higher governance**, including **active** feedback loop



© 2017-2021 OPEN CSIRT FOUNDATION

The authoritative SIM3 assessment tool

<https://sim3-check.opencsirt.org/>



© 2017-2021 OPEN CSIRT FOUNDATION

SIM3 – "O" Parameters

- **0-1 – Mandate**
- 0-2 – Constituency
- 0-3 – Authority
- 0-4 – Responsibility
- **0-5 – Service Description**
- 0-7 – Service Level Description
- 0-8 – Incident Classification
- 0-9 – Participation in Existing CSIRT Frameworks
- **0-10 – Organisational Framework**
- 0-11 – Security Policy

↔ FIRST CSIRT Services Framework

© 2017-2021 OPEN CSIRT FOUNDATION

SIM3 – "H" Parameters



- H-1 – Code of Conduct/Practice/Ethics
- H-2 – Personal Resilience
- **H-3 – Skillset Description** ↔ soon-to-be FIRST roles/competencies doc
- H-4 – Internal Training
- H-5 – (External) Technical Training
- **H-6 – (External) Communication Training**
- H-7 – **External Networking**

© 2017-2021 OPEN CSIRT FOUNDATION

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**

© 2017-2021 OPEN CSIRT FOUNDATION

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**

© 2017-2021 OPEN CSIRT FOUNDATION

SIM3 is neutral



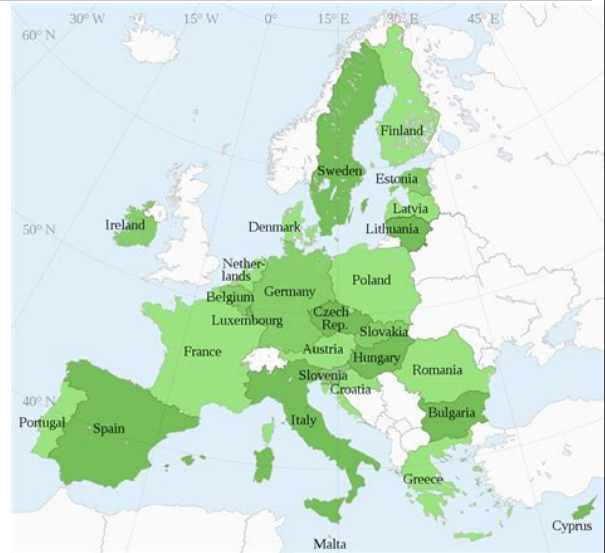
- SIM3 itself is a **neutral** model without prescriptions
 - Exception: 6 parameters have a common sense minimum requirement
 - Example O-7 : human reaction to peer CSIRTs within 2 working days
- Applications of SIM3 can pose demands :
 - Membership criteria (FIRST – this is new)
 - Audit/improvement frameworks (ITU et al.)
 - Accreditations & Certifications (TF-CSIRT Europe)
 - Community frameworks (NCA Japan, CSIRTs Network EU)
 - Anything you choose to define !
- Example application :

© 2017-2021 OPEN CSIRT FOUNDATION

EU NIS Directive



- CSIRTs network
 - 27+ n/g CSIRTs ; ENISA is caretaker
 - Support to increase maturity across the board
 - NIS Directive demands quite high !
- Step-by-step SIM3 based approach towards improving maturity

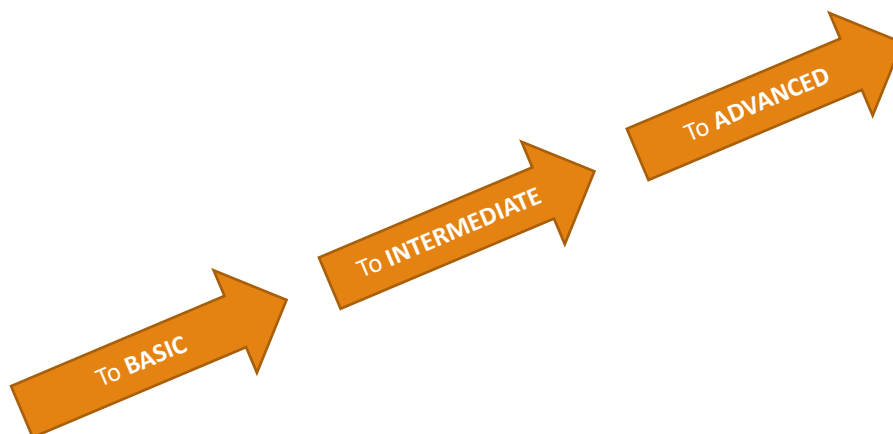


© 2017-2021 OPEN CSIRT FOUNDATION

ENISA approach : for EU national teams



- increasing maturity in 3 steps



© 2017-2021 OPEN CSIRT FOUNDATION

GCMF v2 : for national & governmental teams worldwide



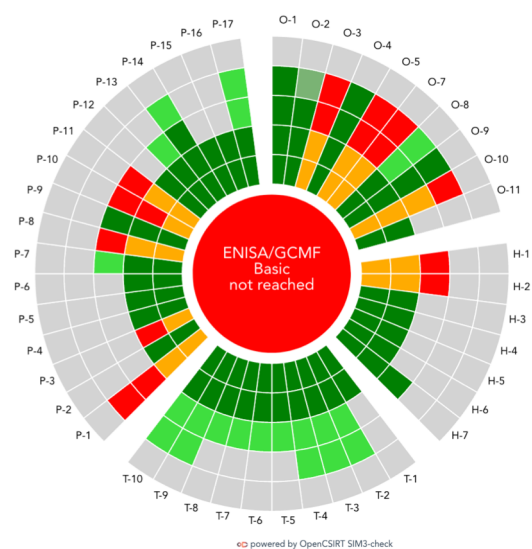
- GFCE & NL initiative – ITU was among the reviewers
- **Identical** to SIM3 & ENISA approach, without EU dimension (v2 version, April 2021)
 - <https://cybilportal.org/tools/global-csirt-maturity-framework/>
- **Could easily be ported to non-national teams**
- And by the way, much recommended too:
- Getting started with a National CSIRT guide
 - <https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/>
 - April 2021
 - GFCE & NL deliverable for GFCE WG-B TF-CIM

© 2017-2021 OPEN CSIRT FOUNDATION

The authoritative SIM3 assessment tool



<https://sim3-check.opencsirt.org/>



© 2017-2021 OPEN CSIRT FOUNDATION

Open CSIRT Foundation maintains and governs SIM3



- SIM3 used by FIRST, ITU, TF-CSIRT, CSIRTs Network, NCA, GFCE, Cyber4Dev, Commonwealth, OAS, LACNIC, WACREN, AfricaCERT and others, including consultancy companies
- The use of SIM3 v1 is free ... but how to maintain SIM3 then ?
- OCF has been given this role and fulfills it, not for profit - **welcomes sponsors**
- Certified SIM3 Auditors, more than 50 now
 - The Auditors help improve SIM3 in workshops every 1-2 years
 - Trainings: 2017 (Japan), 2018 (Lithuania), 2019 (Japan, Cyprus), 2020 → 2021 (Krakow)
 - Auditors do *assessments* and/or *audits*
- SIM3 v2 (due spring 2022) will remain free for non-profit and internal use (and by certified auditors), but will request a contribution fee for *commercial* use
- Good cooperation with FIRST, ITU, TF-CSIRT, NCA, ENISA and others.

© 2017-2021 OPEN CSIRT FOUNDATION

4 example approaches to increase maturity



- Traditional approach: improve maturity per parameter
 - For all 44 parameters
- Improved approach #1: Write at least the following documents :
 - Organisational Framework, covering most O parameters, plus some H and P
 - Staff hiring and development policy, covering most H parameters
 - rfc2350
 - and handle the rest per parameter
- Improved approach #2: Write at least the following documents :
 - A full CSIRT Maturity "handbook" covering all parameters
 - Rfc2350
- ITU is establishing a structured approach for National CIRTs

© 2017-2021 OPEN CSIRT FOUNDATION



Measure and Improve National CIRT Maturity

ITU CyberDrill 2021, 14 October 2021

PRESENTERS: MIROSLAW MAJ & DON STIKVOORT

INFO@OPENCSIRT.ORG

WWW.OPENCIRT.ORG

© 2017-2021 OPEN CSIRT FOUNDATION