



Do You Want to Improve Your Country's or Organisation's Handling of Cyber Security Incidents?

Where to Start.

Don Stikvoort
Cyber4Dev expert
Open CSIRT Foundation, chairman of the board



Who am I : Don Stikvoort

<https://www.first.org/hof/inductees>

*1961

Theoretical physics

Internet & security pioneer in Europe since 1988

Builder of European CSIRT cooperation since 1993

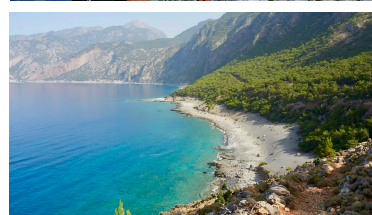
Entrepreneur since 1998

Founding father of NCSC-NL and many more CSIRTs

Author of SIM3 maturity model

Chairman of Open CSIRT Foundation

Cyber4Dev training coordinator & expert



“If you think you’re too small to make a difference, try sleeping in a closed room with a mosquito”.



Incident Management (IM) – not just response



1. Preparation
2. Prevention
3. Detection
4. Resolution, or: Response – the “R” in CERT/CSIRT
5. Lessons learnt – feeds back to the previous 4 items



Funded by the
European Union



What kind of teams are we talking about, really ?



FIRST Framework SIG is working on global typology with only 4 main types (so far):
[simplified characterisations: there’s a thousand shades of green]

- | | |
|-------------------|--|
| 1. CSIRT/CERT/etc | does the whole range of IM (and more) |
| 2. SOC | specialises in detection and is more IT centric – but similar to CSIRT |
| 3. PSIRT | deals with product security: mostly vulnerability management |
| 4. ISAC | CSIRT without doing incident response |

We focus on CSIRT/CERT/SOC here – but an ISAC is close to those.

Oh and by the way an nCSIRT/NCSIRT/NCSC is a CSIRT on steroids, but basically a CSIRT.



Funded by the
European Union



#1 Find Champions & build a human network



Best if you have two:

1. Policy champion
2. Technical champion

Multi-stakeholder approach, first and last

Build a national cyber incident management network, or CSIRTs network – based on **cooperation, collaboration & inspiration** – and well-understood authority

2021 guide, published by the GFCE :

<https://cybilportal.org/publications/getting-started-with-a-national-csirt-guide/>





[same for an organisation or corporation, just smaller scale]

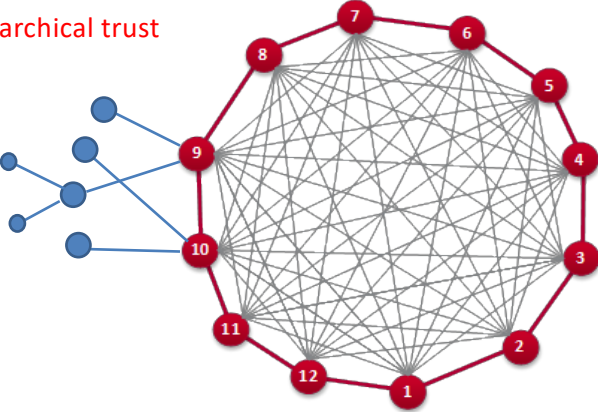



#3 Build trust and maintain it





 #4 How it works worldwide 

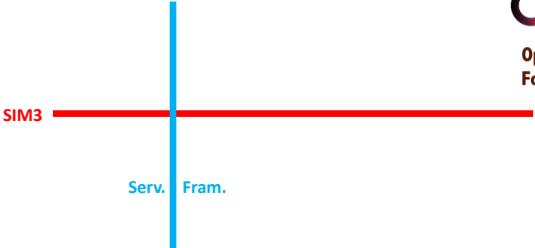
CSIRT System is a mix of non-hierarchical trust relationships and some mostly national structure




 Funded by the European Union

 #5 Use these 

1. SIM3 for overall Maturity
2. FIRST CSIRT Services Framework
3. ENISA or NIST best practices as guide for your Incident Management process
4. CSIRT Services Roles and Competencies (new doc)



 Funded by the European Union



#6 SIM3



Security Incident Management Maturity Model

1 2 3

Online tool: <https://sim3-check.opencsirt.org/> (standard is inside)

45 parameters in 4 categories and 5 maturity levels

Organisation: 11

Human aspects: 7

Tools: 10

Processes: 17

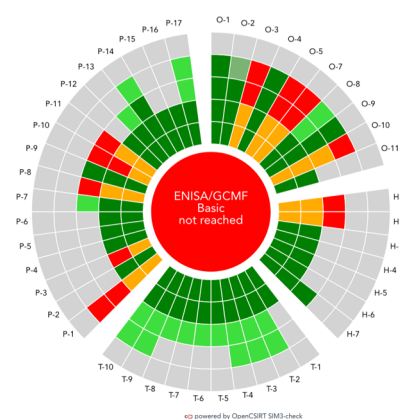
0 = not there

1 = in people's heads only

2 = written down, informal

3 = written down & approved

4 = as 3, but **regularly** assessed on authority of **higher governance**, including **active feedback loop**



Funded by the European Union



#7 FIRST CSIRT Services Framework



v2.1: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

5 Service areas:

- Security Event Management <<< SOC area !
- Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

Every service area has several services defined

Every service has several functions defined



Use as restaurant menu, starting from mandate and available people and resources



#8 Incident Management process



Use either ENISA or NIST IM process :

ENISA: <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>

NIST: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

This is a matter of taste, both are popular.



Funded by the
European Union



#9 Roles and skills



Use the CSIRT Services Roles and Competencies (new doc v0.9):

https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf

This maps from the “FIRST CSIRT Services Framework” services to roles, and from there to skills – both soft and hard skills.

KEEP IT SIMPLE !

A smaller CSIRT only needs a few roles: (senior) incident handler, manager, ...



Funded by the
European Union



#10 Humans are your true capital

CSIRT members need :

1. Communication skills
2. Technical skills and experience
3. Trust building skills → human networks
4. Common sense
5. Creativity, thinking outside the box
6. At times: stamina

INVEST in your team, invest in your people, enable training, participation in CSIRT meetings etc etc



Photo by [roya ann miller](#) on [Unsplash](#)



CYBER4Dev

www.cyber4dev.eu

