



TF-CSIRT

TRANSITS I

Organisational Module

Your trainer: **Miroslaw Maj**

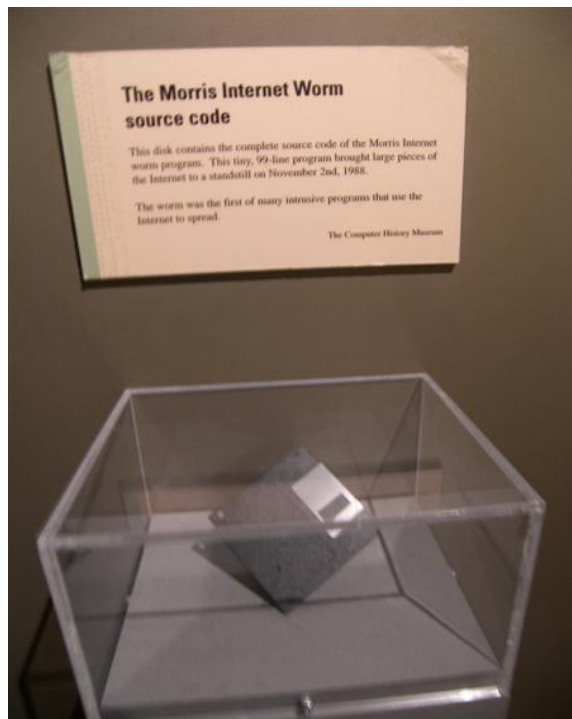
Abuja, Nigeria

December, 2023

Authors: Serge Droz, Jaap van Ginkel & Don Stikvoort

Version: 7.3 draft

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/)









TF-CSIRT

Why CSIRT ?

Why incident management ?

Let's get to know each other some more



TF-CSIRT



What is it you want to protect ?



TF-CSIRT

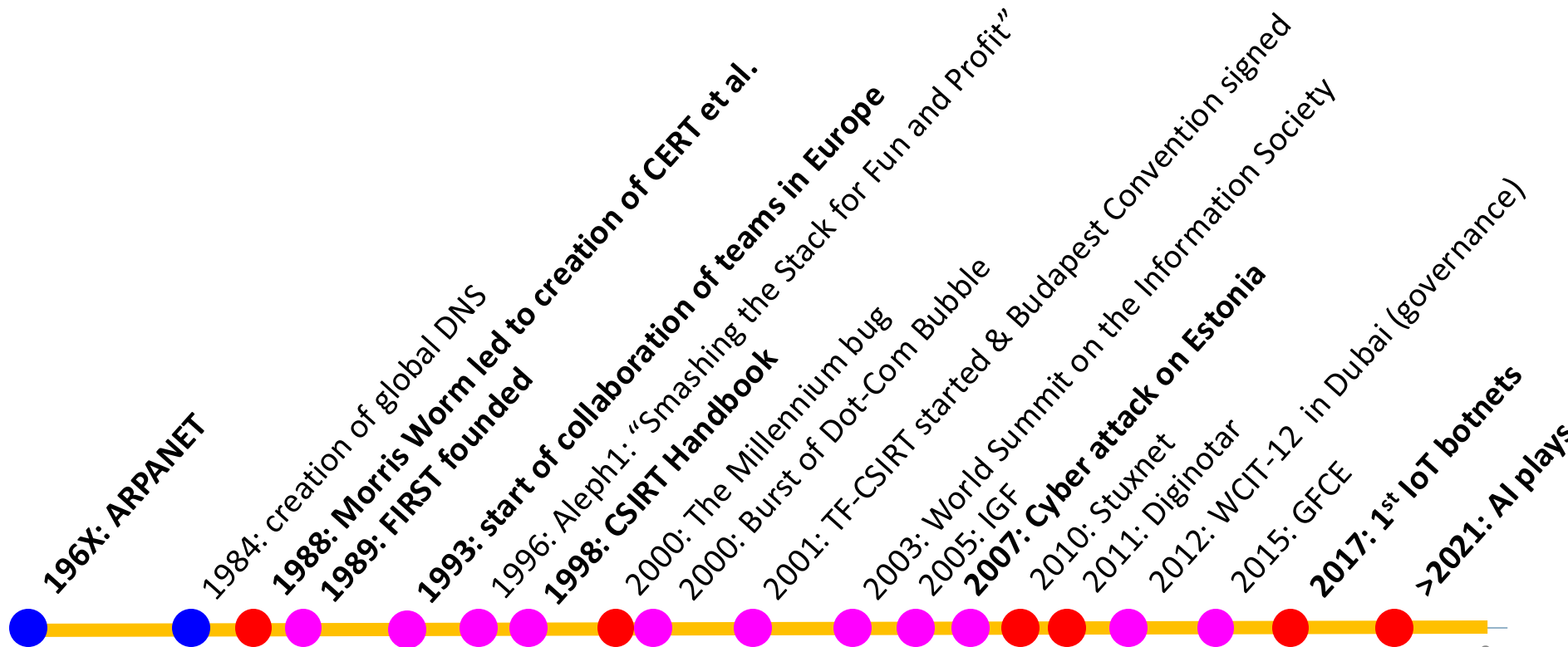
- Groups of 4 :
 - 7 minutes discussion
- Discuss in plenary



Internet history : need for incident management & governance



TF-CSIRT

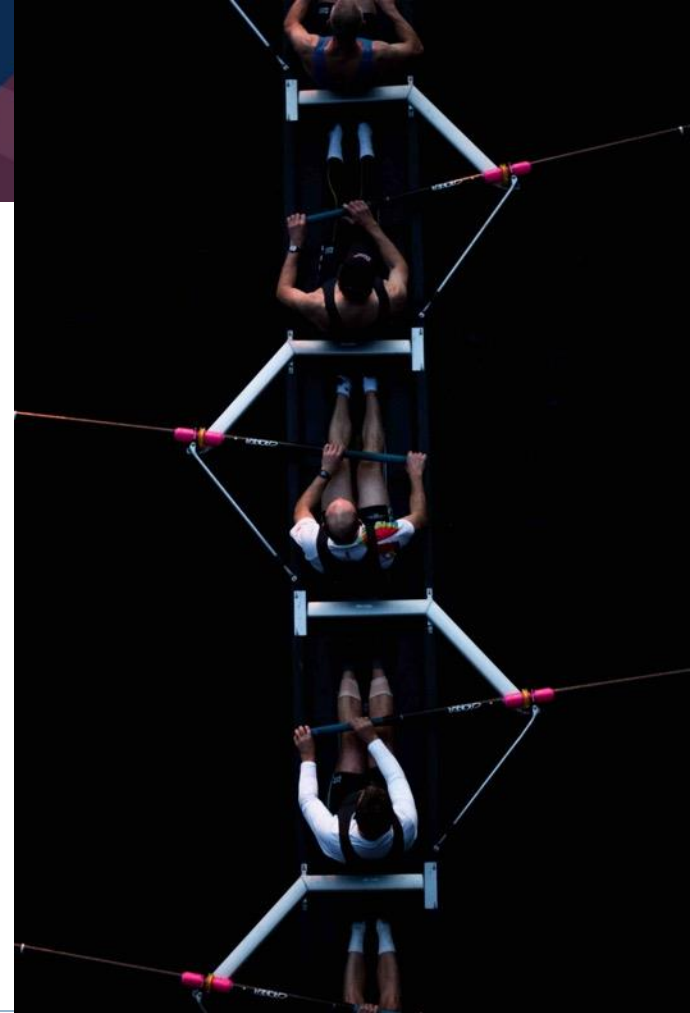


Timeline courtesy FIRST

CSIRT means : to organise incident management

To organise incident management in the CSIRT way means to **organise** :

- IM Awareness on all levels
- Authority
- Escalation
- External Contacts (CSIRTs, police, etc.)





TF-CSIRT

Starting Points

Key references and other starting points

The CSIRT work is a many faceted and challenging craft

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





CERT : Computer Emergency Response Team

- Origin 1988, later trademarked
- CERT Coordination Center (CERT/CC)
- Permission to use : “CERT – Contact CERT/CC Security Operations (security-operations@cert.org) for CERT partnership details” (recent quote from CERT/CC)

CSIRT : Computer Security Incident Response Team

- Origin 1998 : <http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- Free to use !

IHT, SIRT, CIRT, IHC, SOC (a story in itself), etc. etc.

What's in a name – you must have this capability !



SIM3 = **S**ecurity **I**ncident **M**anagement **M**aturity **M**odel

- For (self) assessment,
- membership criteria &
- audit purposes (including Certification)

45 parameters in 4 categories

- O – Organisation : 11
- H – Human Aspects : 7
- T – Tools : 10
- P – Processes : 17



Current is SIM3 v2 interim: see <https://opencsirt.org/csirt-maturity/sim3-and-references/>

SIM3 ctd.

Each parameter can score :

0 = not available / undefined / unaware

1 = implicit : “between the ears only”

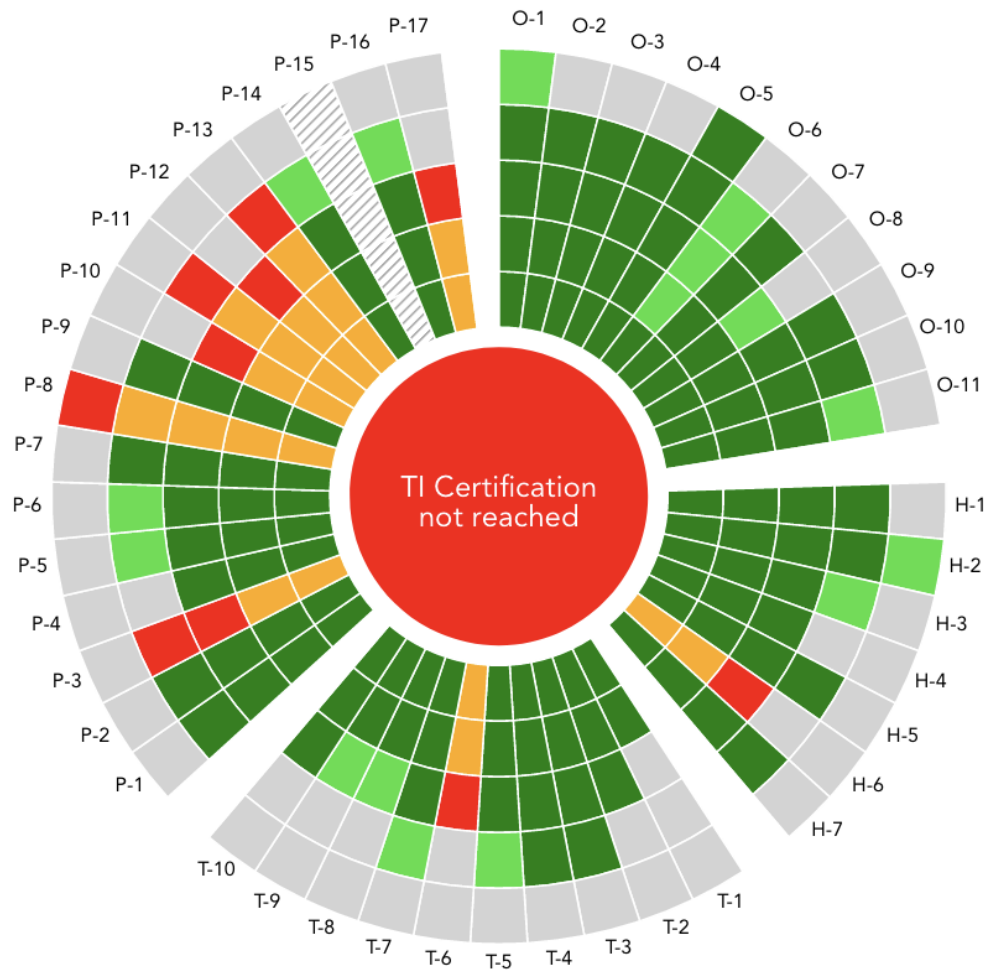
2 = written down but not formalised

3 = like 2 but approved by CSIRT head :
“rubberstamped” (or published)

4 = like 3 but actively assessed or audited
on authority of governance levels above the
CSIRT management on a regular basis

Try this out:

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





FIRST Services Framework v2.1

- https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- Just "CSIRT" in the full name is confusing: it works perfectly for CSIRTs (CERT/CDC/NCSC/etc) but just as well for SOC and ISACs (the FIRST Framework SIG considers dropping "CSIRT" from the name for that reason)

For **product** security teams (PSIRTs) – see

https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

These frameworks enumerate in depth the kind of “services” that an IM team can deliver to their constituencies (their clients)

- This is an amplification of the SIM3 parameter O-5 (and O-7 in regard service levels)
- SIM3 and the service frameworks are “orthogonal”: SIM3 describes the whole range of 45 maturity parameters for a CSIRT – the Services Framework is an in depth survey of the O-5 parameter!



TF-CSIRT

Basics & Exercise

Basic concepts leading into a group exercise

For your CSIRT to make sense you must understand your organisation



TF-CSIRT

Incident management is about your organisation !

- It's **not** primarily about computers, routers and networks
- It **is** about you and your boss and the receptionist and all others, it's about your products and services, it's about your customers and shareholders

Your CSIRT wants to prevent and cure incidents

So you need to know and understand your organisation

- **Hierarchy:** How do units relate? Who is in charge?
- **Maze:** Who are the key people you need to persuade?



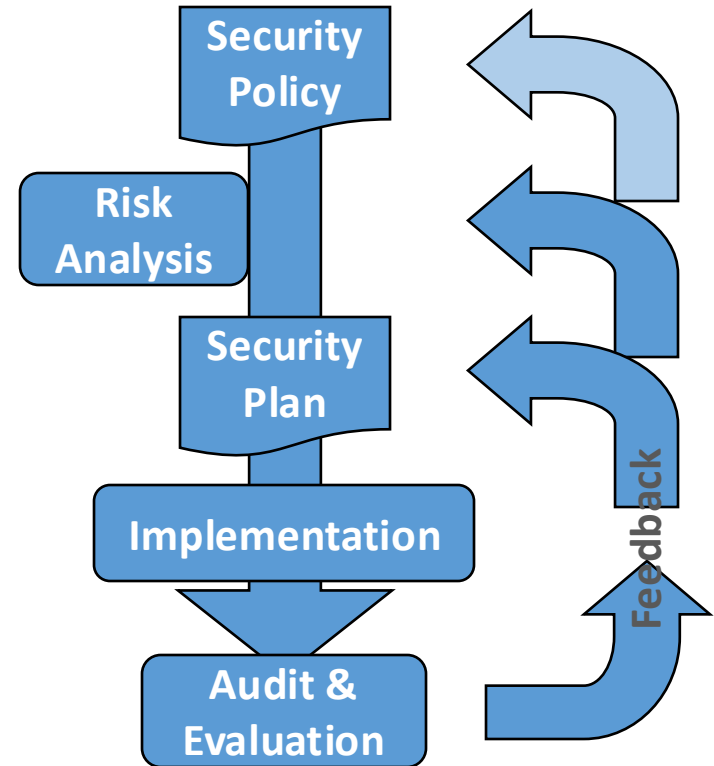


Make sure you implement a cycle like this

- DO the feedback and ensure FOLLOW UP

CSIRT can contribute to ...

- Risk Analysis
- Security Plan
- Evaluation





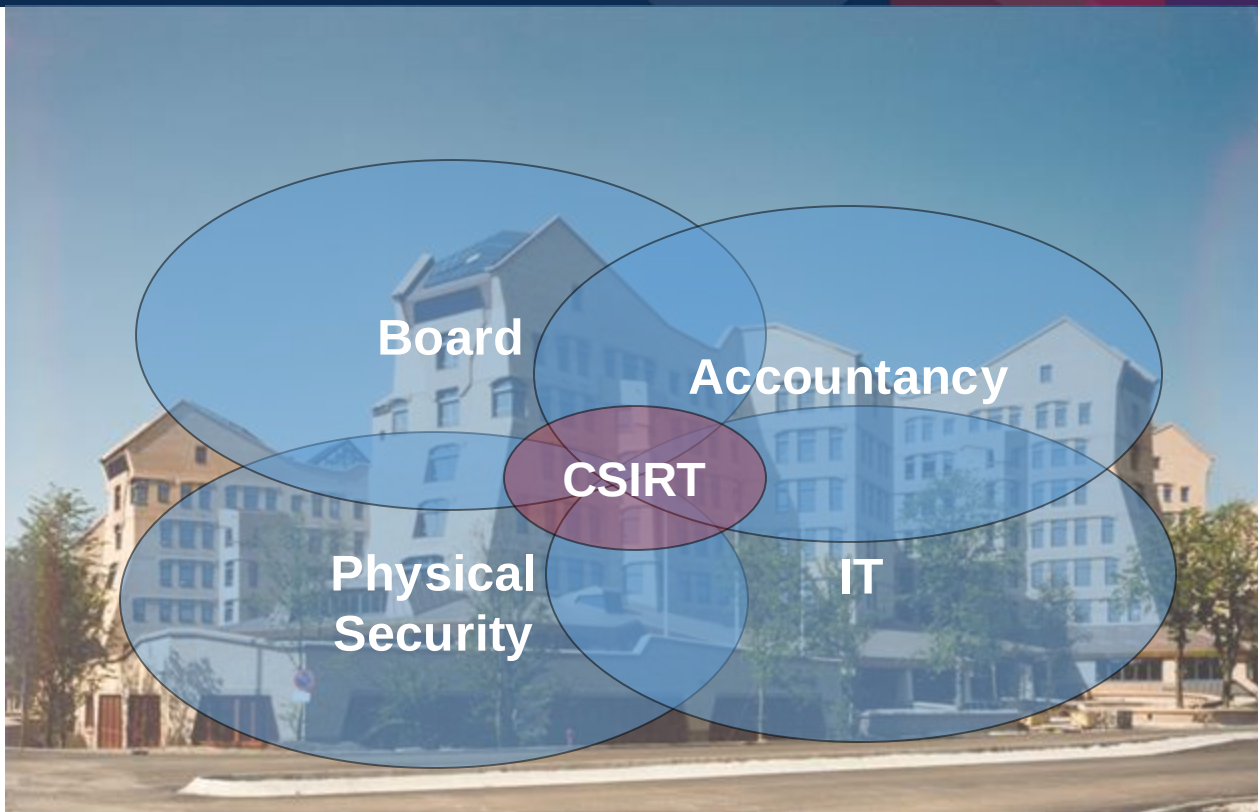
“Security is not a product it is a process” – Bruce Schneier

See security as a holistic challenge – not fragmented

- “integrated security”, “TSM” etc.
- Information security has many actors
 - CISO
 - CSIRT
 - IT department & SOC
- Physical security
- Risk Management
- Crisis Management
- Business continuity Management (BCM)

End-responsible = board / CEO

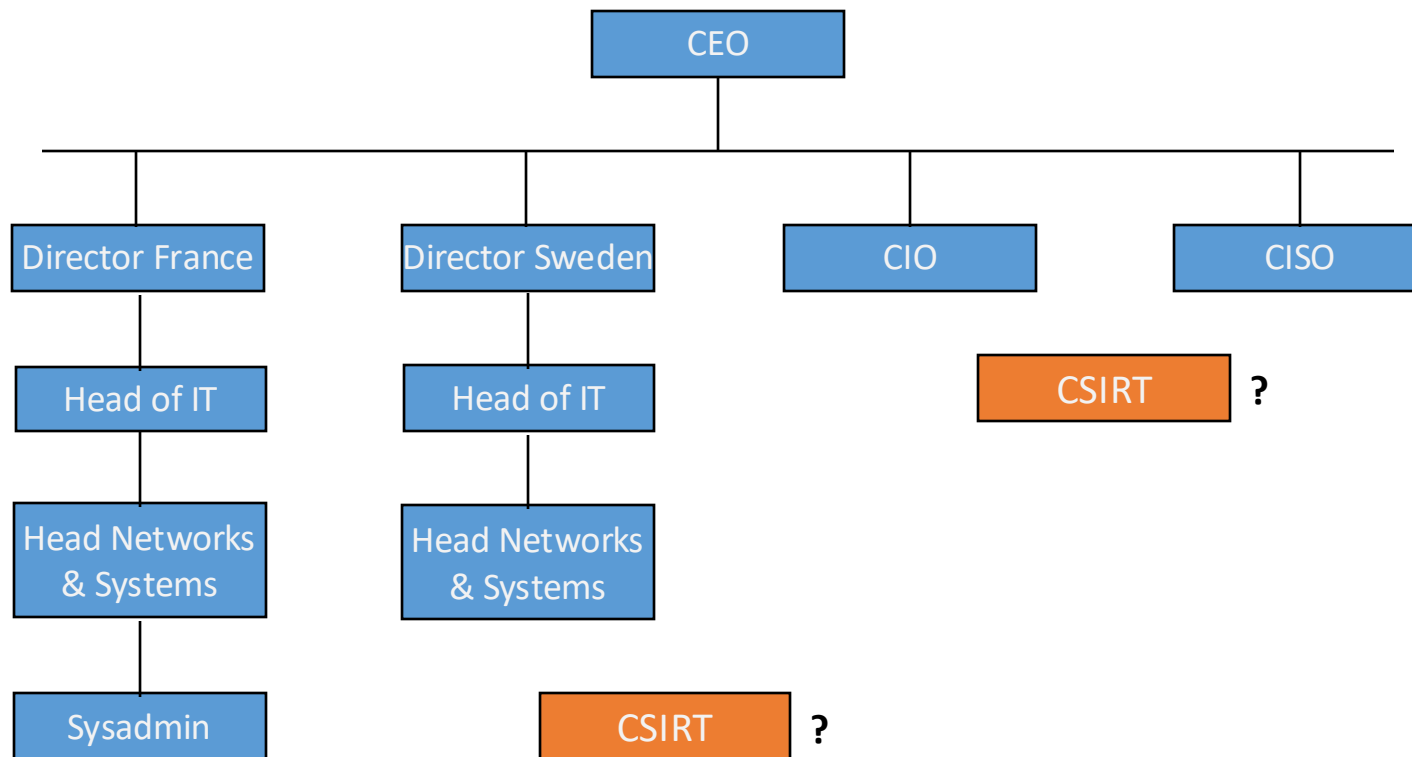




Example: PariSto Bank



TF-CSIRT



Exercise (30 minutes)



TF-CSIRT

- Split into groups of 3-4
- In each group :
 - One member make a few notes for wrap-up
 - Choose **one** of your CSIRTs and **discuss (= exercise purpose)**
 - Mandate : how and by whom was your CSIRT mandated ?
 - Constituency : who do you work for ?
 - Authority : what is your team allowed to do ? What “power” do you have ?
 - Responsibility & Services : what is your team expected to do ? what services does your team offer to the constituency in order to fulfil that responsibility ?
 - Place of team in organisation : where do you fit in ? Does this set-up work well ?
- Plenary wrap-up (discuss **only one** highlight per group discussion)



00 : 07 : 21

>

Change Clock Type

Digital

Duration:

00

07

21

TimeUp Reminder (Optional):

--

--

--

Choose Sound Effect

Tick

Choose TimeUp Sound

Alarm



TF-CSIRT

Organisational Factors

The main organisational factors to bear in mind



CSIRT Mandate should come from Board level

For national teams best anchored in legislation

- And/or national cyber security/resilience policy

Funding also needs to be anchored at high level to ensure continuity



Mandate = SIM3 parameter O-1



Who does your CSIRT work for, what is the target group ?

Main types of constituencies:

- National/CII : serving the country, or at least the critical infrastructure
- Sector : serving a specific sector like e.g. the energy sector (usually inside a country)
- Government
- Military
- Academia : serving universities, research institutes, schools, libraries, etc.
- Own organisation/corporation : most commonly found all over society/business
- Paying customers : offering commercial CSIRT services

PSIRTs (Product Security Incident Response Teams) are special case

Constituency = SIM3 parameter O-2



Authority – what is your team allowed to do

- Advise only ?
- Power of escalation ? - you need that if you can't enforce ...
- Power of enforcement ? (e.g. blocking)

Authority must come from highest governance level (not from head of IT)

- Have a “CSIRT charter” document approved and rubberstamped
- CISO role is intermediary between CSIRT and Board

Authority is not the key factor to success, but it can help.

Al Capone: a gun and a good argument is better than just a good argument !

Authority = SIM3 parameter O-3



reactive :

- **Incident handling**
- Alerts & warnings
- Vulnerability handling
- Artifact handling

pro-active :

- Announcements
- Technology watch
- Audits/assessments
- Tools maintenance
- Security tool development
- Intrusion detection

quality management :

- Risk analysis
- Business continuity planning
- Security consulting
- Awareness building
- Education/training
- Product evaluation/certification

No team is responsible for all of these !

Responsibility = SIM3 parameter O-4



FIRST Services Framework: works for CSIRT etc / SOC / ISAC

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

Service areas: (subdivided in services and then functions)

- Security Event Management – the SOC area
- Incident Management – the traditional CSIRT area
- Cyber Threat Intelligence Management – making sure you are not blind and deaf
- Vulnerability Management – more specialised, only few teams do this in full
- Knowledge Transfer – at least part of this is essential for any and all IM teams

rfc2350 : strong advice to fill it out

- Operational factsheet of your CSIRT (services and contact data)
- Place publicly on your team's webpages in your native language and English

Service description = SIM3 parameter O-5



- 
1. Incident prevention
 - Awareness raising, audits, port and vulnerability scans, advisories, ...
 2. Incident detection
 - IDS sensors, firewall alerts, point-of-contact, ...
 3. Incident resolution
 - Incident co-ordination, on site handling, ...
 4. Incident quality management
 - Team meetings, lessons learnt, recommendations, ...
 - Feeds back to incident prevention



Incident Management : essential function for any CSIRT

- May consist of any or all of :
 - Incident response coordination
 - Incident response support
 - Incident response on site
 - Incident analysis
 - Forensic evidence collection
 - Tracking

However ... always remember to establish **lessons learnt** and feed them back to **incident prevention**





When is the service provided ?

- 24/7 : expensive & only useful when also applies to IT operators
- Office hours only : 09 to 17, 08 to 20 or similar
- Out of hours coverage
 - For emergencies only (who decides?)
 - **Best effort is always better than no effort**

Other service levels

- Probably dependent on incident classification !
- (Human) reaction time
- Resolution time : be **very** careful

Service level description = SIM3 parameter O-7



How do you classify incidents ? (= taxonomy)

- Classical taxonomies focus only on incident types.
A good example is the popular eCSIRT.net / ENISA taxonomy :
https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md
- More modern approaches also take impact/cost (and/or priority) into account.
See e.g. https://www.first.org/resources/guides/csirt_case_classification.html

Classification can be used for reporting, planning (including writing processes) and for service levels

Incident classification = SIM3 parameter O-8



Participation in CSIRT systems = SIM3 parameter O-9



Public media policy = SIM3 parameter O-6



Typically a formal approach

- ISO27001
- National standard
- NIST Cybersecurity Framework

Preferably (also) have your own CSIRT security policy

- CSIRT has special needs
- Testing, port scanning
- Honeypot
- Extra fallback facilities
- Make sure to cover BCM !!



Security policy = SIM3 parameter O-11



Write a charter (organisational framework) for your CSIRT

- Essential to clearly define your CSIRT and prevent discussions when incidents happen
- High level description
 - Mandate, constituency, authority, responsibility, services, structure & place of team
- “CSIRT Handbook” is good background material :
<https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305>
- Real life example :
Ask Open CSIRT Foundation for a (free) word template (info@opencsirt.org – template will go publicly online early 2024)

Organisational framework = SIM3 parameter O-10



Central (most common)

- CERT-BDF (serving Banque de France)
- ThaiCERT (serving Thailand: government & national)
- MSCERT (Microsoft PSIRT: in Redmond)

Distributed

- SURFcert (serving SURF, Dutch NREN)
- TeliaCERT and “sub-CERTs” (serving Telia Company ISP & telco operator)

Timezone distributed (very rare)

- Cisco PSIRT (Cisco’s product security team) “follows the Sun”



Most common : part of IT department

- Remember : CSIRT is a spaceship
- Mission and authority must be anchored at highest governance level
- Ensure good working relationships & direct escalations with :
 - Your constituents e.g. through established contacts in all departments
 - Line management (your boss)
 - Highest governance level e.g. through CISO
 - PR staff (press contacts)
 - Legal department & privacy officer

Sometimes : organisation support function

- Great place to be for mandate, authority and escalations
- But: leave your ivory tower !



TF-CSIRT

Human Factors

The main human/personnel factors to bear in mind

Exercise (30 minutes)



TF-CSIRT

- Split into same groups of 3-4 as before
- In each group :
 - One member makes a few notes for wrap-up
 - Choose **one** of your CSIRTs and **discuss (= exercise purpose)**
 - What challenges do you face in meeting your requirements for staffing ?
 - Do you know the skillset for the staff you need and have appropriate job descriptions ?
 - Is there a policy for hiring and developing CSIRT staff ? So not just generic ?
 - Do you have access to technical training / training budget for your staff ?
 - Can you get apart from technical training also training in “soft skills” ?
 - Can you effectively escalate (also outside business hours) to a) your own boss, b) the higher governance levels, c) the press handlers, d) your corporate lawyer(s) ?
- Plenary wrap-up (discuss **only one** highlight per group discussion)

Without a good, trustworthy team ... nothing goes



TF-CSIRT

The human factor is the prime factor in the success of any CSIRT

Trust is one of the key factors in successful CSIRT cooperation

- **Your CSIRT takes at least a year to build trust and can lose it overnight**
- Trust is built on personal relationships, not on organizational ones
- Avoid hiring ex(?) -crackers
- Use a Code-of-Conduct and discuss it with your team each year : e.g.
<https://www.trusted-introducer.org/TI-CCoP.pdf> or <https://ethicsfirst.org/>

TLP - Traffic Light Protocol : active knowledge and use required : <https://www.first.org/tlp/>

Code of Conduct = SIM3 parameter H-1



Need enough team members to cover for holidays/illness

- SIM3 says **minimum** 3 (can also be part-timers)
- Burnt-out team members are not effective

Always have a plan B (discussion)

CSIRT work can be challenging – what to compensate

- Offer appropriate rewards
- Keep work varied
- Budget for trainings
- Let staff attend events

Staff resilience = SIM3 parameter H-2



What skillsets are needed?

- General: common sense, communication, diplomatic, quick learner, stress resistant, team player, integrity, owns up to mistakes, problem solving, time management, ...
- Technical: to match what the CSIRT offers

Skillset description for each job profile

- (Senior) incident handler, researcher, general manager, ...
- Save yourselves time by using the final draft of FIRST's "CSIRT Roles and Competences":

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

Need other resources ?

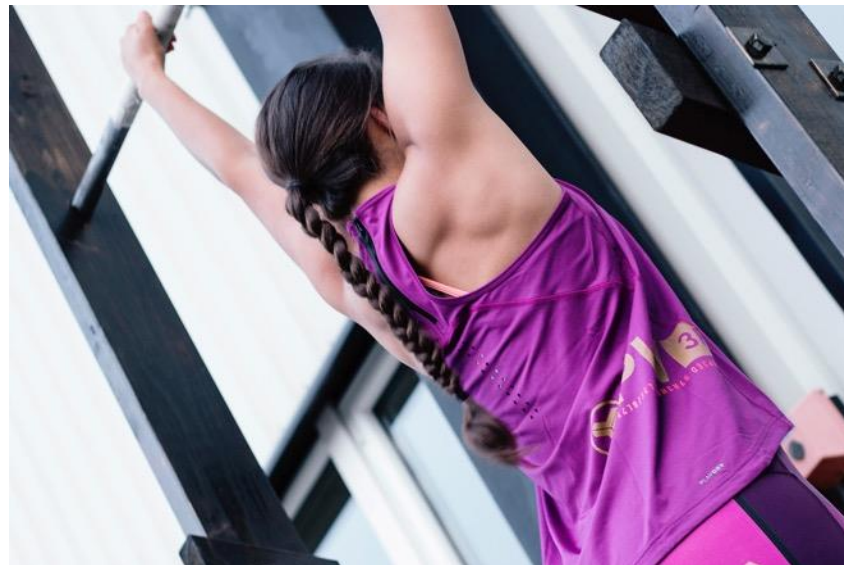
- Specialist skills (e.g. forensics), legal, crisis management, ...
- Arrange **before** an emergency hits

Skillset description = SIM3 parameter H-3



Team & Personal development plan(s)

- Skills development: include soft skills
- Budget & timeline
- Feedback : commonly done by manager but consider having an experienced team member do feedback instead (less pressure, more coaching style)



Staff development = SIM3 parameter H-4
Technical training = SIM3 parameter H-5
Soft skills training = SIM3 parameter H-6

THE MEANING OF COMMUNICATION
IS
THE RESPONSE YOU GET
(= the result)





TF-CSIRT

Wrap-up





Stay visible for your constituency (also when you rock !)

- Presence on internal web pages (security, helpdesk)
- Regular newsletters, workshops once or twice per year

Stay visible for Board and management

- Quarterly and annual reports
- War stories and statistics : add cost savings figures if possible

Stay visible for the world

- Memberships of trusted fora
 - Your favourite national forum
 - Your favourite regional forum (TF-CSIRT, APCERT, **TBA**, etc.)
 - FIRST : <http://www.first.org/>
- Go out there : meeting face-to-face is essential for building web-of-trust and to help develop your team's abilities



90% of your time can easily be wasted on 10% of the question. Prioritise, discuss with colleagues, focus on the desired outcome and damage control – incident handling is not scientific research.

“Habe Mut, dich deines eigenen Verstandes zu bedienen.” – have the courage to use your own mind ! (Immanuel Kant, 1724-1804)

Read some blog(s) and articles, e.g. Bruce Schneier, Brian Krebs et al.

Take nothing for granted, not even from *Famous Name* or your trainers here – or from your colleague who has done this work for 15 years : YOUR idea may be the difference that makes the difference



- NCSC-NL cyber security assessments :
<https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents>
 - Various reports: we all suffer from security incidents
- Annual cost of global cybercrime
 - Symantec: \$110 billion in 2012
 - McAfee: \$ 600 billion in 2017
 - Forbes: expected to reach \$ 2 trillion by 2019
<https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6b99128b3a91>
- “Insider Threats as the Main Security Threat in 2017”
<https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/>
- Your suppliers/partners may be the **weakest link**



TF-CSIRT

**Thank you !
Any Questions ?**

Don.Stikvoort@opencsirt.org

Authors: Serge Droz, Jaap van Ginkel & Don Stikvoort

Version: 7.3 draft

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/)