TF-CSIRT

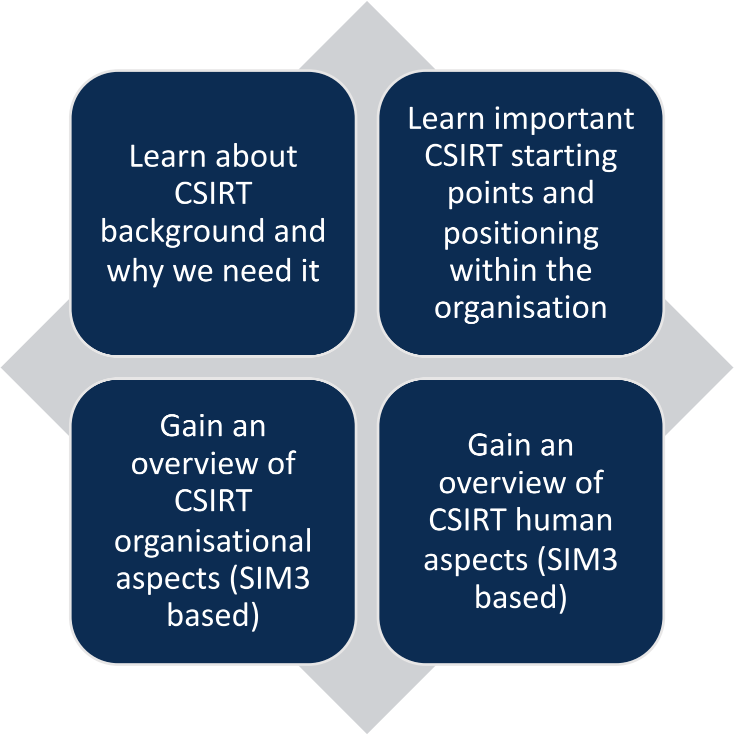
TRANSITS I

Organisational Module

Authors: Serge Droz, Jaap van Ginkel, Sigita Jurkynaitė & Don Stikvoort

Version: 7.2 (full update by Sigita Jurkynaitė & Don Stikvoort, Nov’23-May’24)

Learning Objectives



Learn about CSIRT background and why we need it

Learn important CSIRT starting points and positioning within the organisation

Gain an overview of CSIRT organisational aspects (SIM3 based)

Gain an overview of CSIRT human aspects (SIM3 based)

Session Plan

TF-CSIRT

- Why CSIRT ?
- Starting Points & Basics
- Basics & Exercise
- Organisational Factors
- Human Factors
- Wrap-up

TF-CSIRT

Why CSIRT ?

Why incident management ?

Let’s get to know each other some more

Photo by [Jeffrey Lin]() on [Unsplash]()

What is it you want to protect ?

Groups of 4 :

- 7 minutes discussion

Discuss in plenary

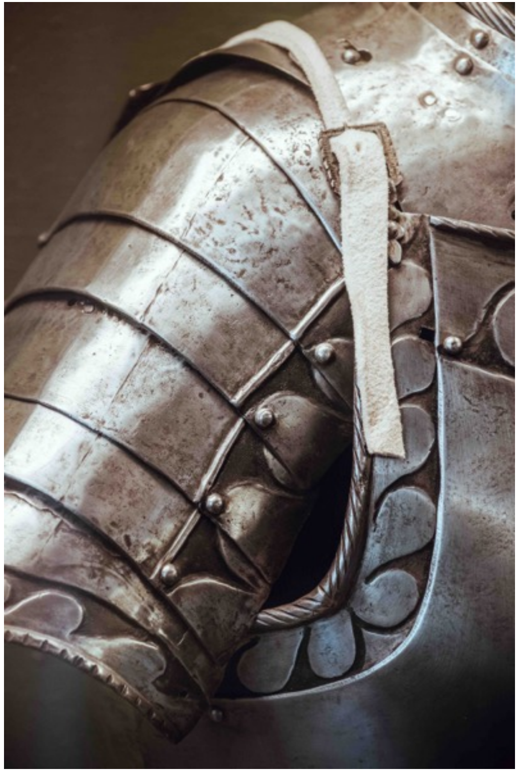
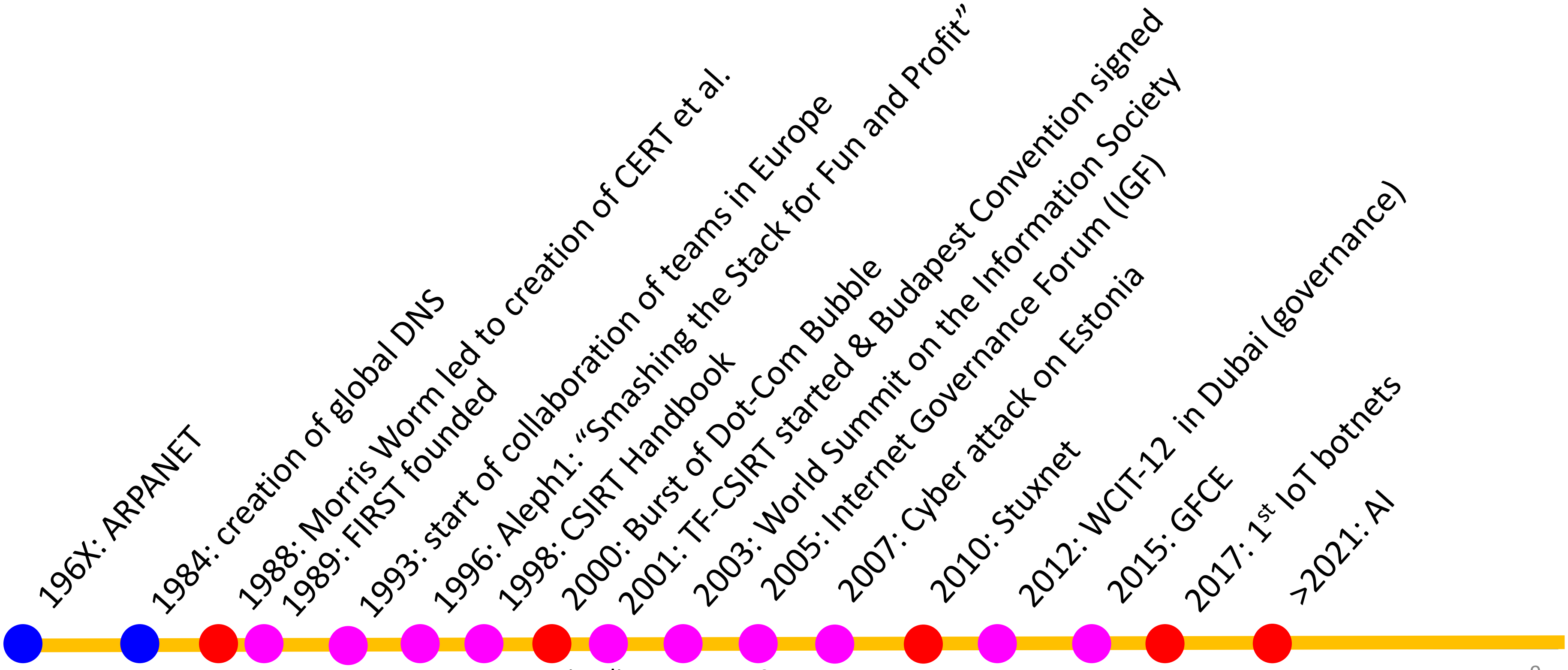


Photo by Samuel Zeller on Unsplash

Internet history : need for incident management & governance



196X: ARPANET

1984: creation of global DNS

1988: Morris Worm led to creation of CERT et al.

1989: FIRST founded

1993: start of collaboration of teams in Europe

1996: Aleph1: “Smashing the Stack for Fun and Profit”

1998: CSIRT Handbook

2000: Burst of Dot-Com Bubble

2001: TF-CSIRT started & Budapest Convention signed

2003: World Summit on the Information Society

2005: Internet Governance Forum (IGF)

2007: Cyber attack on Estonia

2010: Stuxnet

2012: WCIT-12 in Dubai (governance)

2015: GFCE

2017: 1st IoT botnets

>2021: AI

Timeline courtesy Serge Droz

Do you have a choice ?

Can you choose not to deal with security incidents ?

Do you like to react more than to prevent ? Do you just love to fight fire ?

So you agree that incident **management** is the way to go

We refer to ourselves in that community as “CSIRTs“: would you prefer to use a term no one understands ?

➔ You need a CSIRT capability to manage incidents

This module is there to help you :

- make your CSIRT fit your local needs
- make your team more effective

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.)

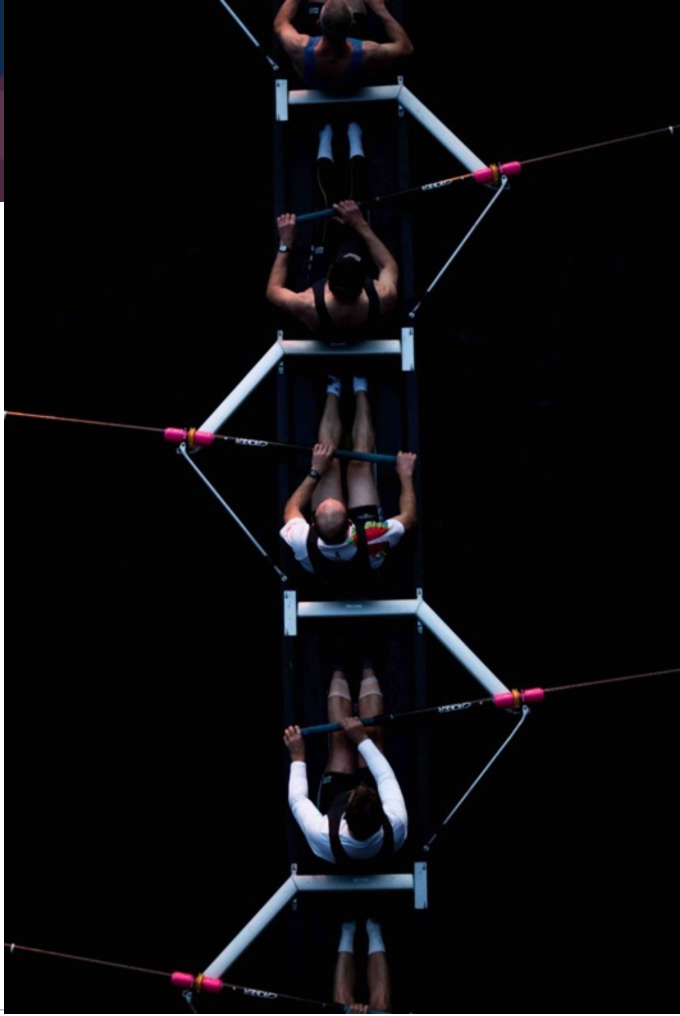


Photo by Josh Calabrese on Unsplash

TF-CSIRT

Starting Points

Key references and other starting points

Starting point #1 : human

The CSIRT work is a many faceted and challenging craft

CSIRT members need :

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

Photo by roya ann miller on Unsplash

Question

TF-CSIRT

What is the difference between CERT and CSIRT ?

Starting point #2 : terminology

CERT : Computer Emergency Response Team

- Origin 1988, later trademarked, but only in the USA and Canada
- CERT Coordination Center (CERT/CC)
- Recommend to nicely ask: “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 as has never been claimed, and now near impossible to “own” the term

nCSIRT, gCSIRT, NCSC, IHT, SIRT, CIRT, IHC …. all CSIRTs

ISAC: like a CSIRT that does analysis and sharing, but no actual response/coordination

SOC: similar to a CSIRT but specialises on the detection element

PSIRT: vendor team, specialises on fixing vulnerabilities in the *ware that they sell

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

Question

Is an nCSIRT or NCSC very different from other CSIRTs ?

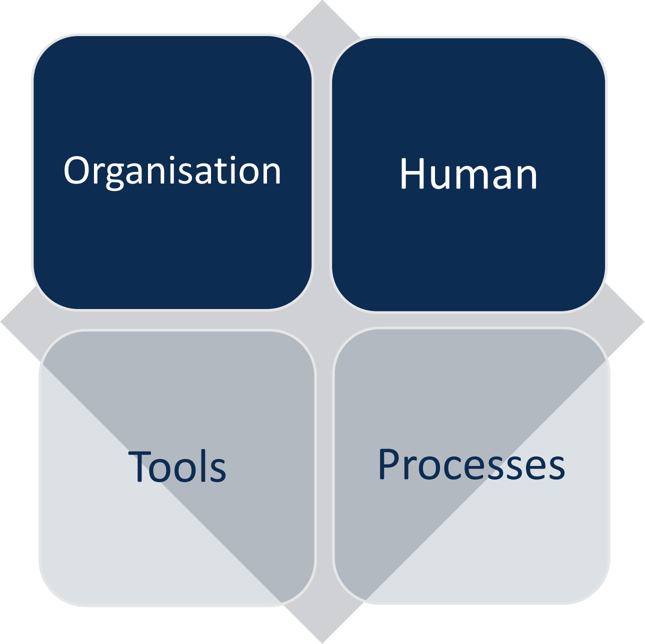
Starting point #3 : SIM3

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 on these Levels:

0 = not available / undefined / unaware

1 = implicit : “between the ears”, not written

2 = written down but not formalised (draft)

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

4 = like 3 but actively controlled/**audited** on authority of **governance levels above the CSIRT management** on a **regular** basis (*or* in national law explicitly)

Try this out: https://sim3-check.opencsirt.org

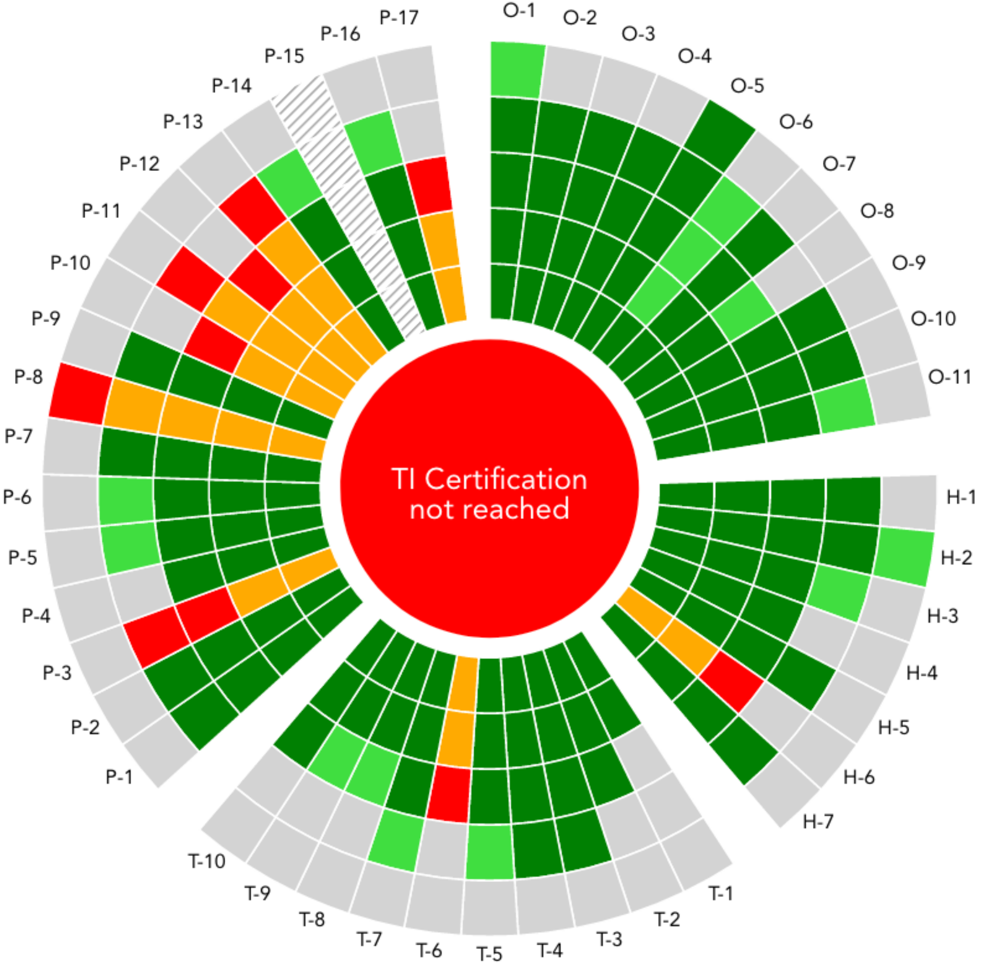


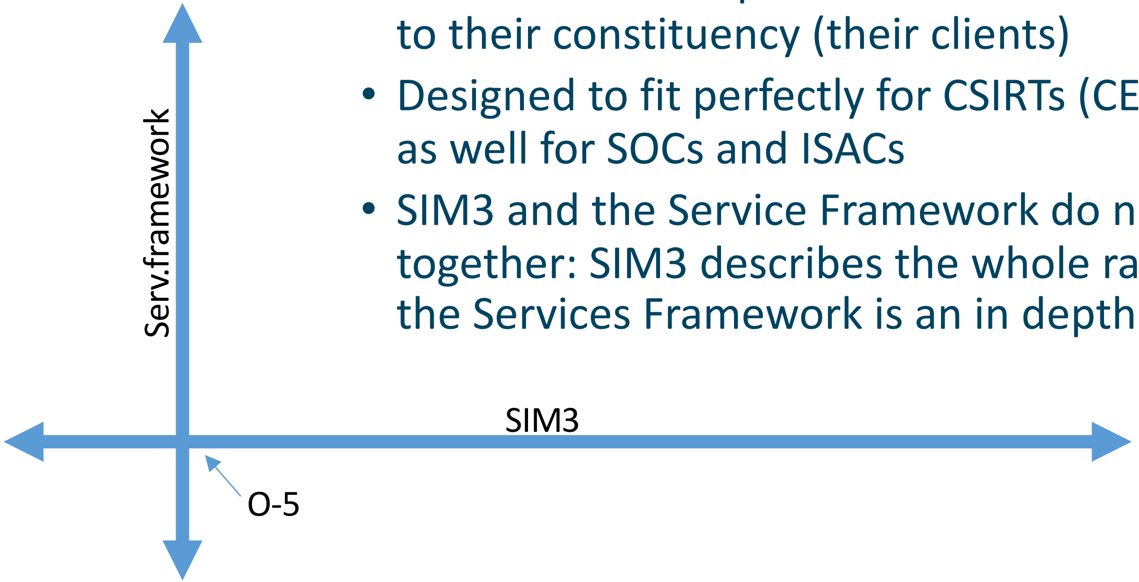
Diagram courtesy OCF

Starting point #4 : FIRST CSIRT/SOC/ISAC Services Framework

FIRST Services Framework v2.1

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

- Enumerates in depth the kind of “services” that an IM team can deliver to their constituency (their clients)
- Designed to fit perfectly for CSIRTs (CERT/CDC/NCSC/etc) but works just as well for SOCs and ISACs
- SIM3 and the Service Framework do not compete but go perfectly together: SIM3 describes the whole range of 45 maturity parameters – 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

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 some of the key people you need to persuade?

Photo by Larisa Birta on Unsplash

Organisation of security

"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, etc.
- Physical security
- Business continuity Management (BCM)
- Risk Management
- Crisis Management

End-responsible = board / CEO / Minister / …

Photo by María Noel Rabuñal Cantero on Unsplash

Security Management Cycle

TF-CSIRT

Make sure you implement a cycle like this

- DO the feedback and ensure FOLLOW UP

CSIRT can contribute to …

- Risk Analysis
- Security Plan
- Evaluation

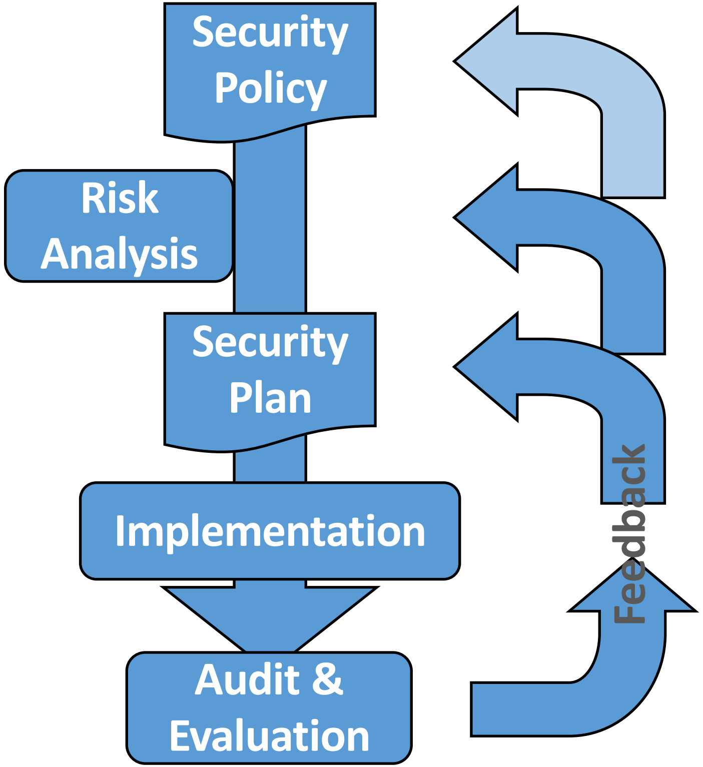


Diagram courtesy S-CURE

CSIRT as spaceship

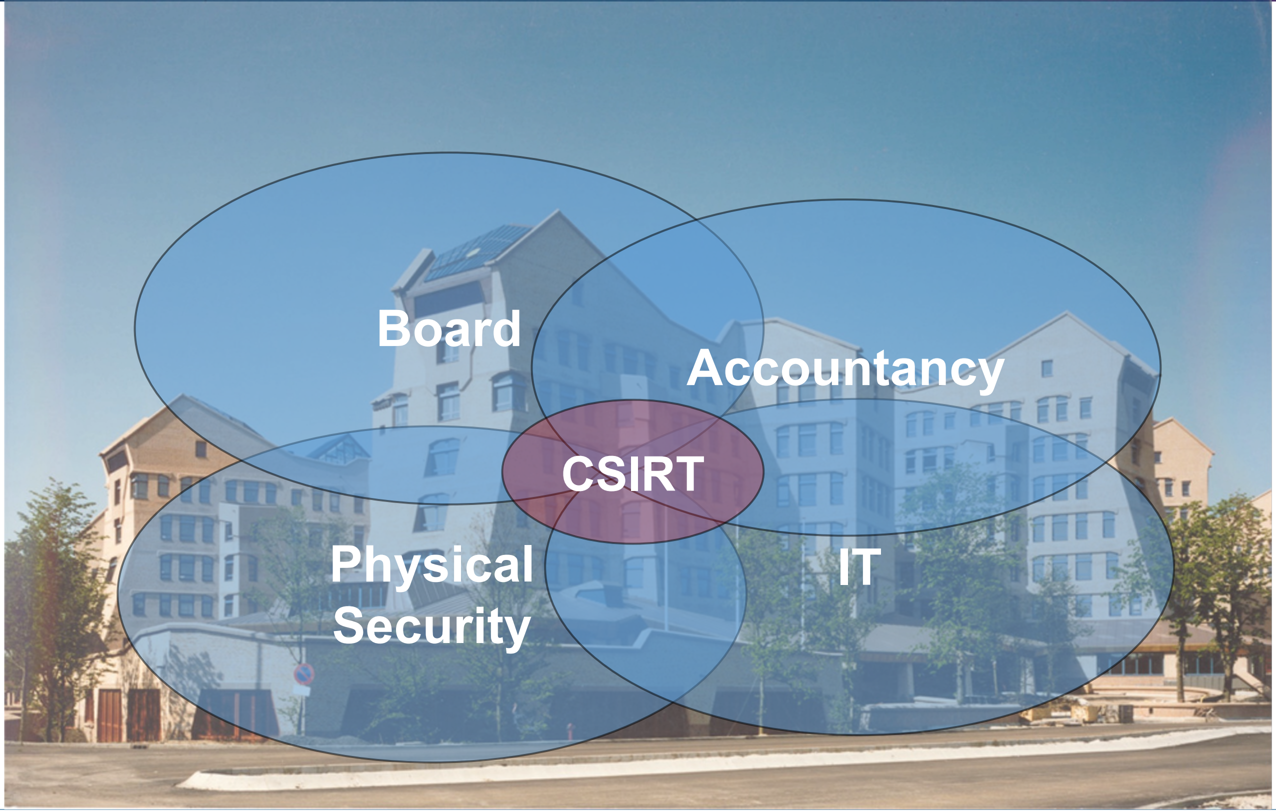


Diagram courtesy OCF

Example: PariSto Bank

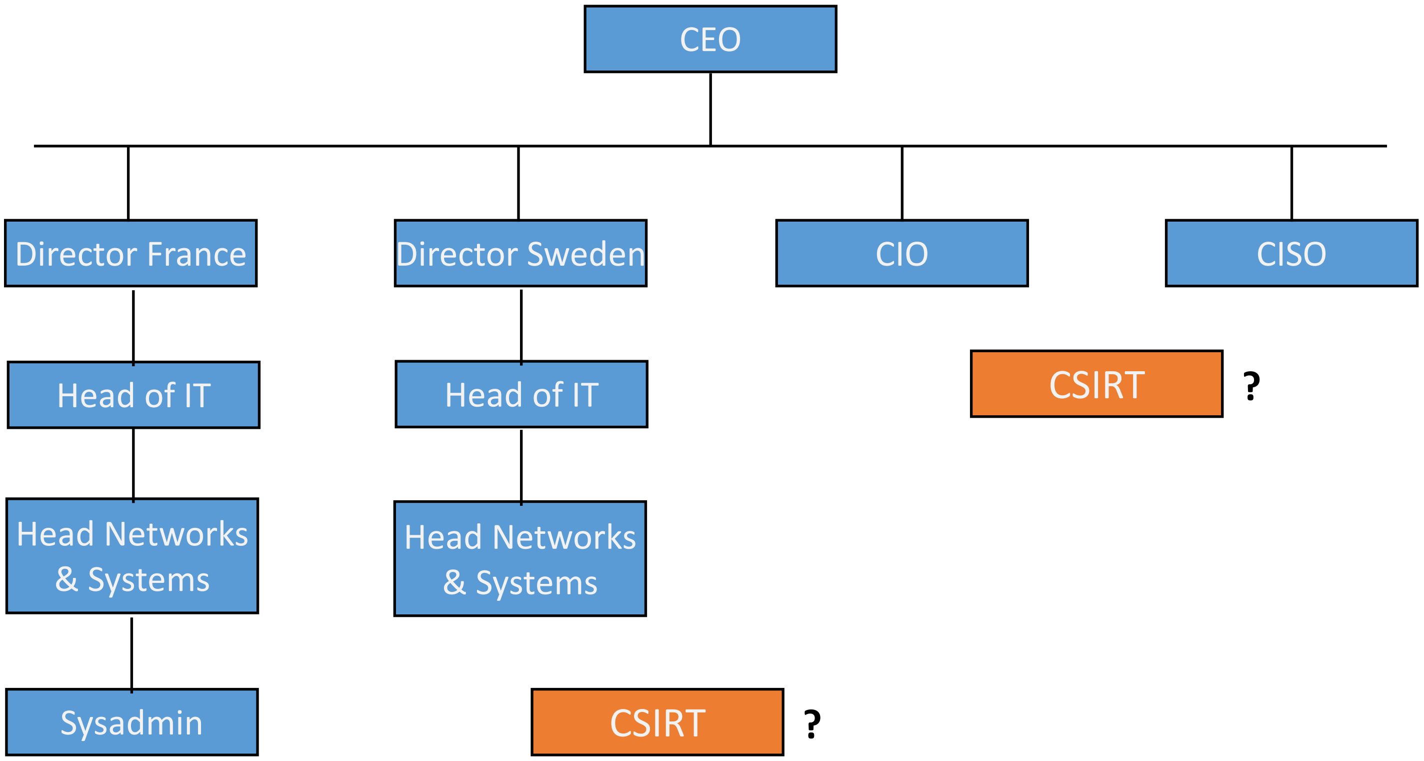


Diagram courtesy S-CURE

Exercise (30+ minutes)

- Split into groups of 3-4
- In each group :
- 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)

TF-CSIRT

Organisational Factors

The main organisational factors to bear in mind

Mandate (SIM3 O-1)

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

Photo by Simon Matzinger on Unsplash

Constituency (SIM3 O-2)

TF-CSIRT

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

Main types of constituencies:

- National/CI : 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

Authority (SIM3 O-3)

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 ☺

Responsibility (SIM3 O-4)

reactive :

- **Incident handling**
- Alerts & warnings
- Vulnerability handling
- Artefact 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 !

List from CERT/CC and ENISA : https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

Services (SIM3 O-5)

TF-CSIRT

FIRST Services Framework: works for CSIRT etc / but also for SOC and ISAC

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

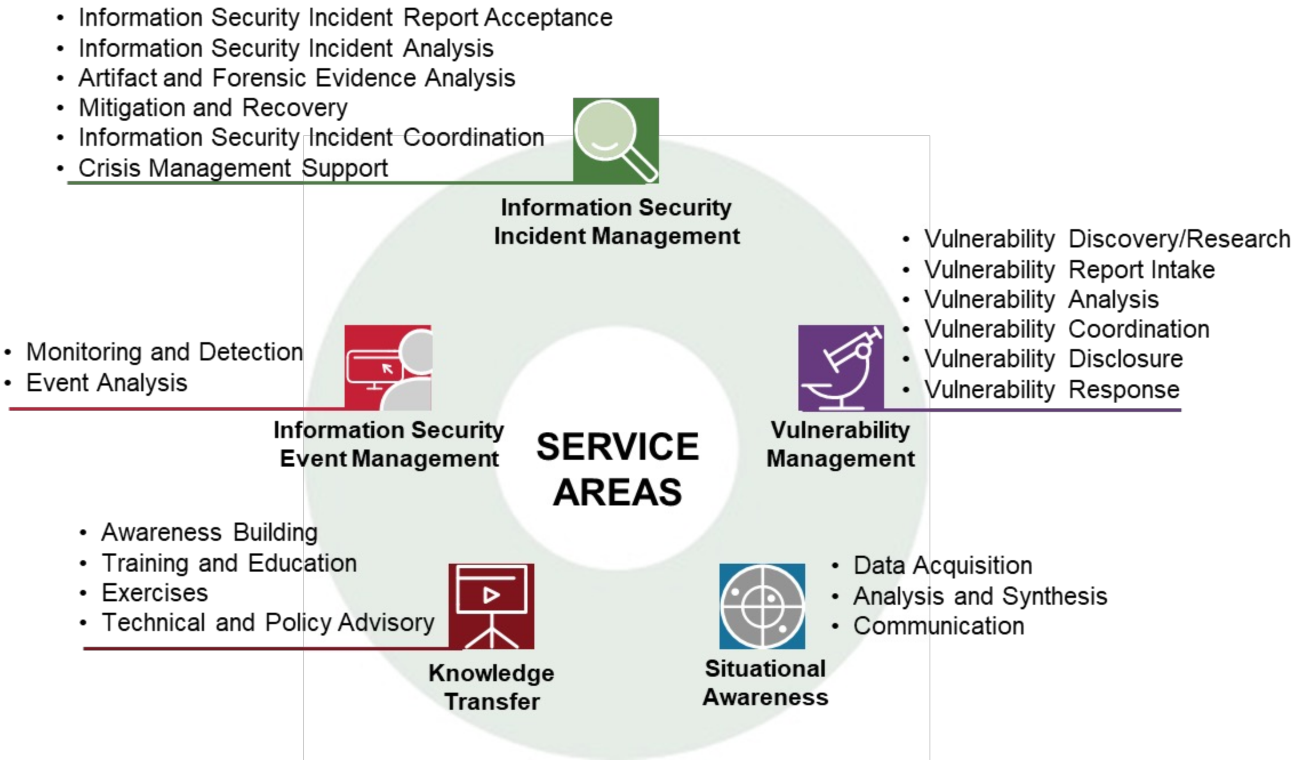
Service areas: (subdivided in services and then functions)

- InfoSec Event Management – the traditional SOC area
- InfoSec Incident Management – the traditional CSIRT area
- Vulnerability Management – more specialised, only few teams do this in full
- Situational Awareness – making sure you are not blind and deaf
- 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

FIRST Services Framework: Service Areas and Services (Functions left out)



SERVICE AREAS

Information Security Incident Management

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

Vulnerability Management

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Information Security Event Management

- Monitoring and Detection
- Event Analysis

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

CSIRT core service(s)

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

Photo by John Cameron on Unsplash

IM Service cycle

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

PSIRT core service

PSIRTs deal with broken things

FIRST **PSIRT Services Framework** recommends starting with:

- Vulnerability Management Policy (as covered in ISO30111)
- Information Handling Policy (as covered in ISO/IEC 29147)
- Vulnerability Scoring/Prioritization Policy
- Remediation Service Level Agreement
- Vulnerability Disclosure Policy (usually a public documentation)

See https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

Public Media Policy (SIM3 O-6)

Do you have a communication department who talk to Radio, TV, newspapers etc. directly? Are you involved to avoid “nonsense”?

What about social media? Which ones do you handle?

Not all media mean well !

Photo by Onur Binay on Unsplash

Photo by Matt C on Unsplash

Service levels (SIM3 O-7)

TF-CSIRT

Most basic one: 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

Incident classification (SIM3 O-8)

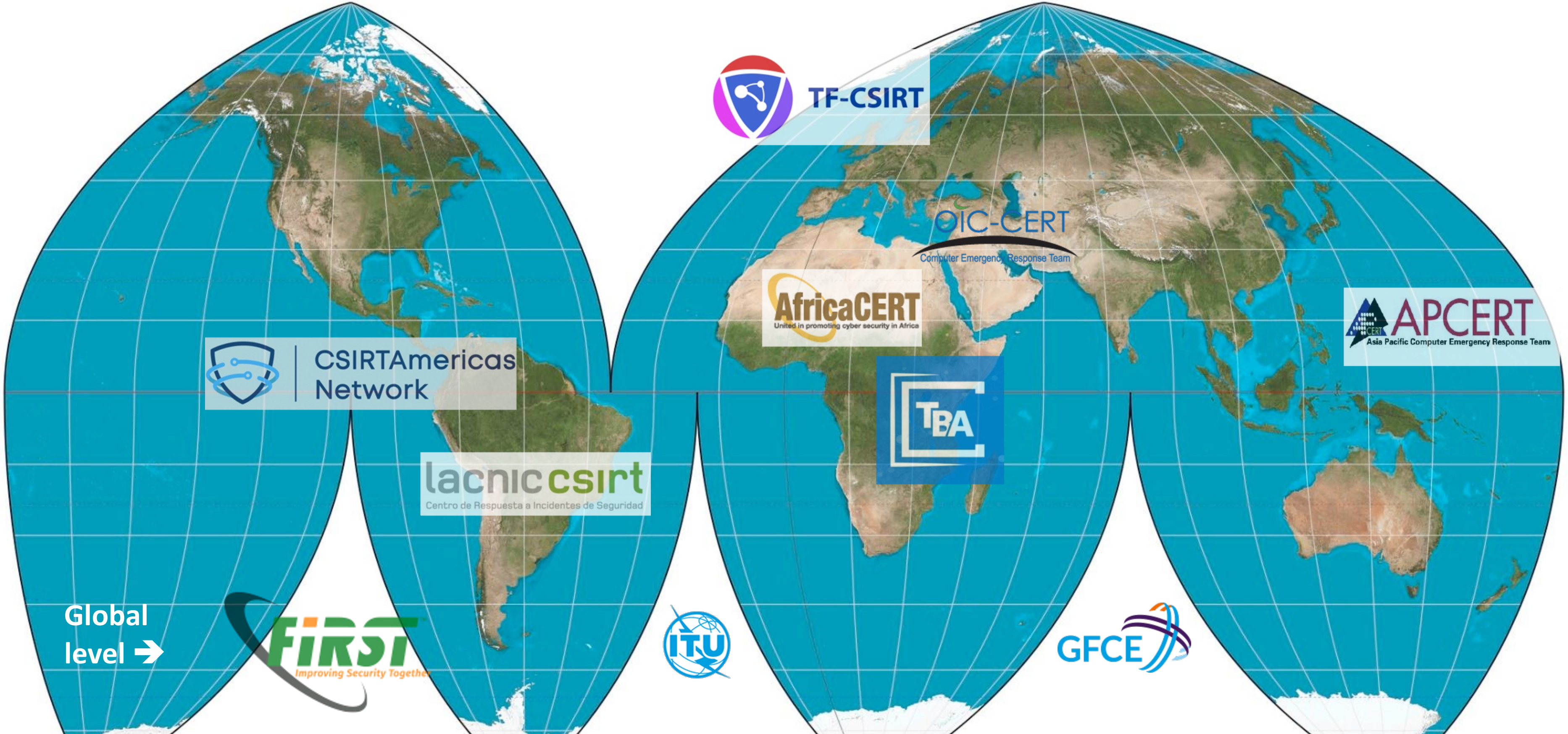
How do you classify incidents ? (= taxonomy)

- Classical taxonomies focus only on technical incident types.
  The ENISA taxonomy is a good example and also used in MISP and other tools:
  https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md
- Internally oriented approaches also take the *impact* of an incident/event into account. Possibly also the *priority*.
  - KISS! Limit the number of classes of *impact* as much as possible, say to max 2 or 3.
  - If you also add *priority*, KISS is even more important.
  - If you don’t, you end up with lots of complexity for your service levels and processes.

Classification can be used for service levels, reporting, writing IM processes, …

Interesting paper:
https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf

Participation in CSIRT systems (SIM3 O-9)


TF-CSIRT
OIC-CERT
Computer Emergency Response Team
AfricaCERT
United in promoting cyber security in Africa
APCERT
Asia Pacific Computer Emergency Response Team
CSIRTAmericas Network
TBA
lacnic csirt
Centro de Respuesta a Incidentes de Seguridad
FIRST
Improving Security Together
ITU
GFCE

Global level →

CSIRT charter (SIM3 O-10)

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://insights.sei.cmu.edu/library/handbook-for-computer-security-incident-response-teams-csirts/
- Example NCSC-NL : https://english.ncsc.nl/publications/publications/2019/juli/02/operational-framework-and-rfc2350

Charter ctd : structure of team

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)

Charter ctd : place of team in organisation

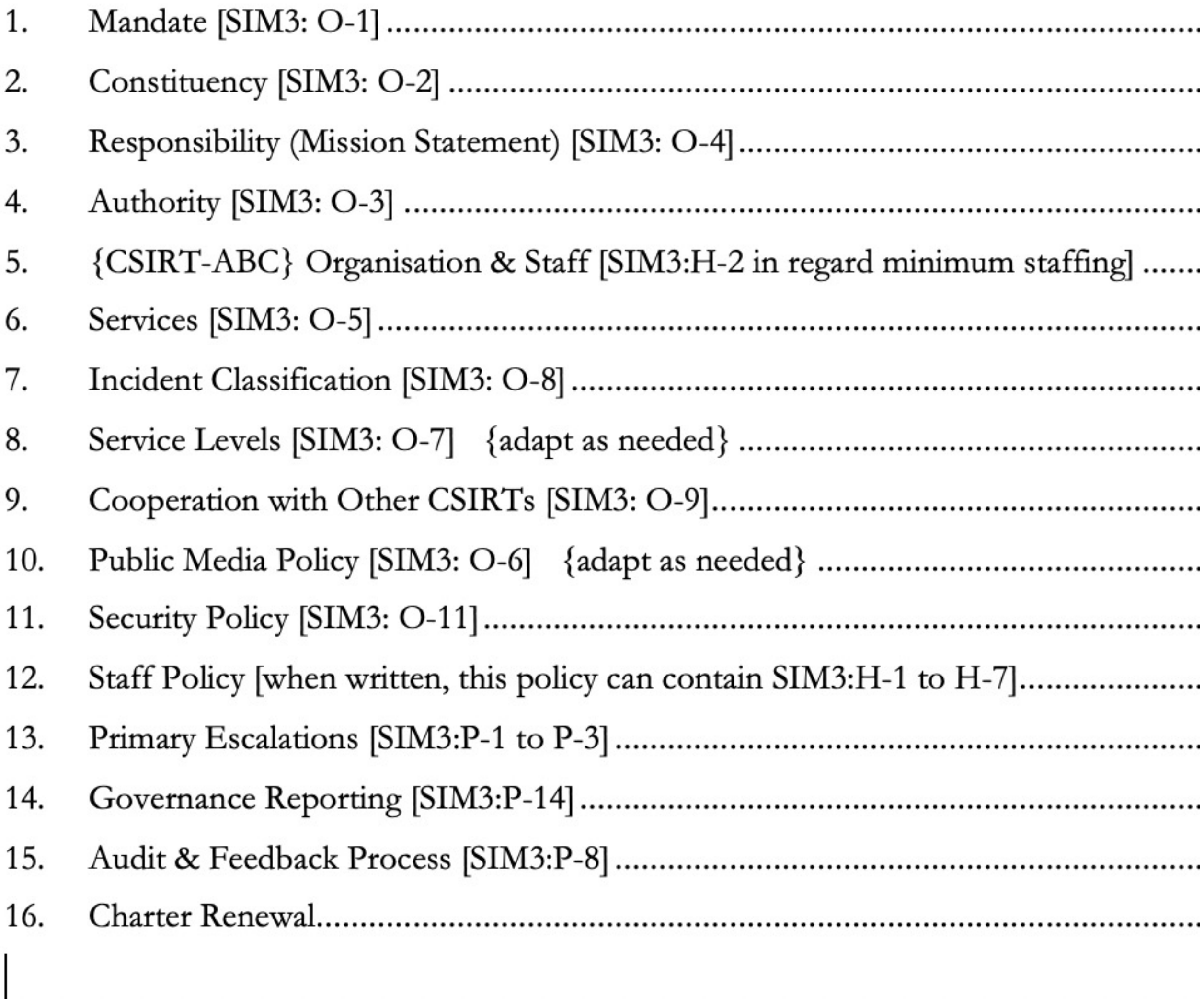
Most common : part of IT department

- Remember : CSIRT is a spaceship
- Mission and authority must be anchored at highest governance level
- Ensure good working relationships & direct escalations with :
  - Your constituents, through established contacts in all entities of the constituency
  - 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 !

Charter example ToC



Security Policy (SIM3 O-11)

TF-CSIRT

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 !

Photo by Ahsan S. on Unsplash

TF-CSIRT

Human Factors

The main human/staff factors to bear in mind

Exercise (15 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” ?
- Plenary wrap-up (discuss **only one** highlight per group discussion)

Code of Conduct (SIM3 H-1) & TRUST

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 organisational ones
- Make sure you hire people that not only you trust, but other teams will trust too (think twice about hiring ?former? Blackhats)
- 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/

Staff Resilience (SIM3 H-2)

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

Skillset (SIM3 H-3)

TF-CSIRT

What skills 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 time by using FIRST’s “CSIRT Roles and Competences”, based on the FIRST Services Framework:

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

- Or consider: https://infosecskillsmatrix.com/rolesskills

Need other resources ?

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

Staff development (SIM3 H-4) &
Technical and Soft Skills training (SIM3 H-5 and H-6)

TF-CSIRT

Team & Personal development plan(s)

- Staff development policy, including all aspects (SIM3 H-4)
- Specific focus on skills development: technical (H-5), but also include “soft skills” (H-6)

  Soft skills are not soft at all

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

Photo by Martine Jacobsen on Unsplash

Prime “soft” skill: human communication

THE MEANING OF COMMUNICATION

IS

THE RESPONSE YOU GET

(= the result)

Photo by Icons8 team on Unsplash

External networking (SIM3 H-7)

Photo by Mapbox on Unsplash

SIM3 O-9 asks for participation in the national and global CSIRT cooperation(s)

SIM3 H-1 asks for trust building

All of that requires that team members **go out** and “network” with others:

- In the constituency
- In the memberships
- Trainings, drills, meetings

TF-CSIRT

Wrap-up

Stay in the picture

TF-CSIRT

Stay in touch with your constituency (SIM3 P-13 and P-15)

- Presence on internal web pages (security, helpdesk), newsletters
- Workshops, trainings once or twice per year
- Visits, meetings

Stay visible for board and management (SIM3 P-14)

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

Stay visible for the world (SIM3 O-9, H-7 and P-17)

- Membership of trusted fora
    - Your favourite national forum
    - Your favourite regional forum (TF-CSIRT, APCERT, etc.)
    - FIRST : http://www.first.org/
- Go out there : meeting face-to-face is essential for building web-of-trust and to get better

Solving the puzzle takes …

Photo by Benjamin Zanatta on Unsplash

90% of your time can be wasted on 10% of the question. Prioritise, brainstorm, focus on the desired outcomes – IM is not science. 10 or 20% of the puzzle pieces may give you enough to control the damage!

*Have the courage to use your own mind**: take nothing for granted, not even from *Insert Famous Name* or an old and wise colleague : YOUR idea may be the difference that makes the difference.

* Immanuel Kant, 1724-1804.

Stay informed

TF-CSIRT

[(Brian) Krebs on Security]

[The Hacker News]

[Dark Reading]

[We Live Security]

[Troy Hunt – Weekly Updates]

[Red Team Notes]

[(Bruce) Schneier on Security]

[Risky Business]

[Black Hills Information Security]

[SANS Daily]

[Re-thinking the Human Factor]

Photo by Matthew Guay on Unsplash

Photo by Convertkit on Unsplash

Reading List

- SIM3 standard: https://opencsirt.org/csirt-maturity/sim3-and-references/
- SIM3 online maturity tool & ENISA baselines: https://sim3-check.opencsirt.org/
- FIRST Services Framework: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- RFC2350: https://www.ietf.org/rfc/rfc2350.txt
- ENISA Reference Incident Classification Taxonomy: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
- FIRST website: https://www.first.org/
- TF-CSIRT Trusted Introducer website: https://www.trusted-introducer.org/
- CSIRT Handbook: https://insights.sei.cmu.edu/library/handbook-for-computer-security-incident-response-teams-csirts/
- NCSC-NL cyber security assessments: https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents
- Cost of cybercrime: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6b99128b3a91
- Insider threat: https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/

TF-CSIRT

TRANSITS I

Organisational Module

The End.

Any questions ?

Authors: Serge Droz, Jaap van Ginkel, Sigita Jurkynaitė & Don Stikvoort

Version: 7.2 (full update by Sigita Jurkynaitė & Don Stikvoort, Nov’23-May’24)