



**TF-CSIRT**

## **TRANSITS I**

### **Organisational Module**

Your trainer: firstname lastname

Location cityname, country

Date dd mon year

**Authors: Serge Droz, Jaap van Ginkel & Don Stikvoort**

Version: 7.2

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

# Learning Objectives



Gain an overview of elements to establish a CSIRT

Discuss where a CSIRT sits within an organisation

Know how to get started

Understand key reference documents to help you





**TF-CSIRT**

**Why CSIRT ?**

**Why incident management ?**

Let's get to know each other some more



TF-CSIRT



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

# What is it you want to protect ?



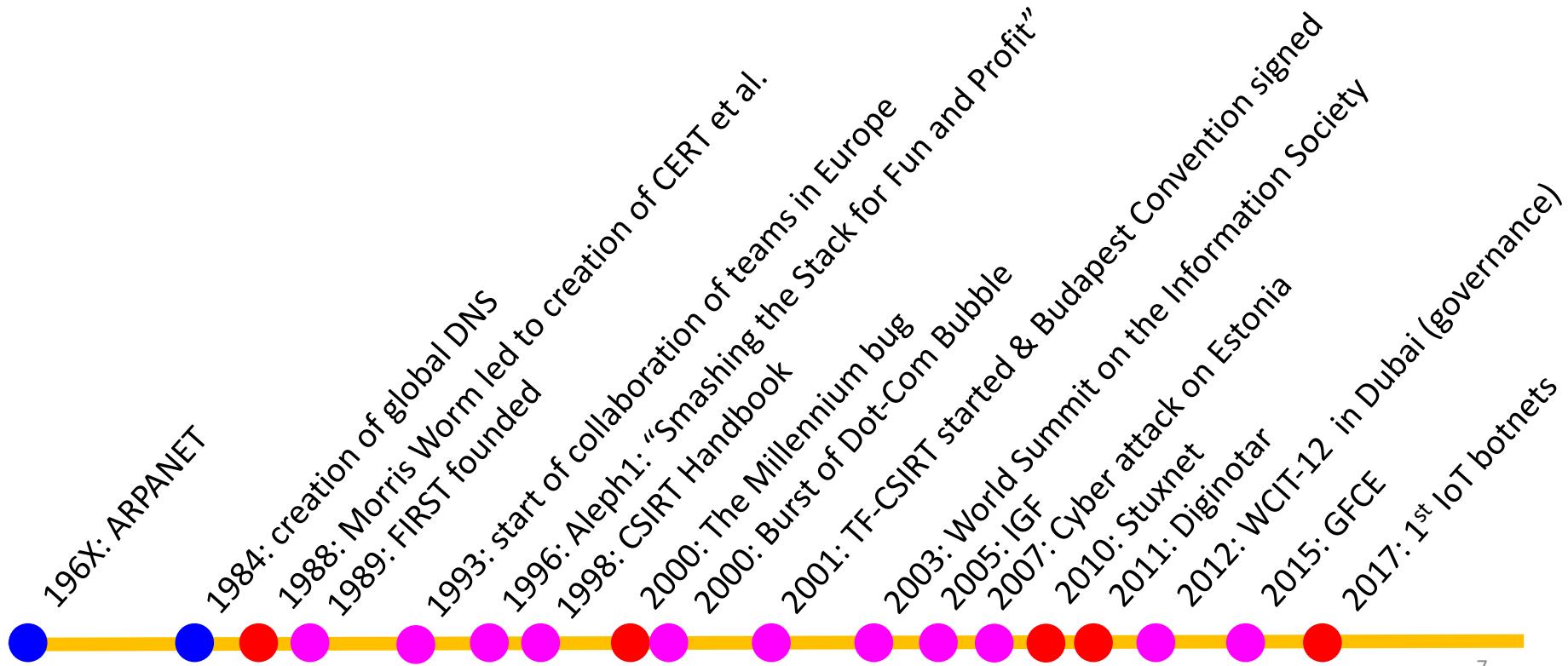
- Groups of 4 :
  - 7 minutes discussion
- Discuss in plenary



# Internet history : need for incident management & governance



TF-CSIRT



## Do you have a choice ?



TF-CSIRT

- 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 do 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



TF-CSIRT

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

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

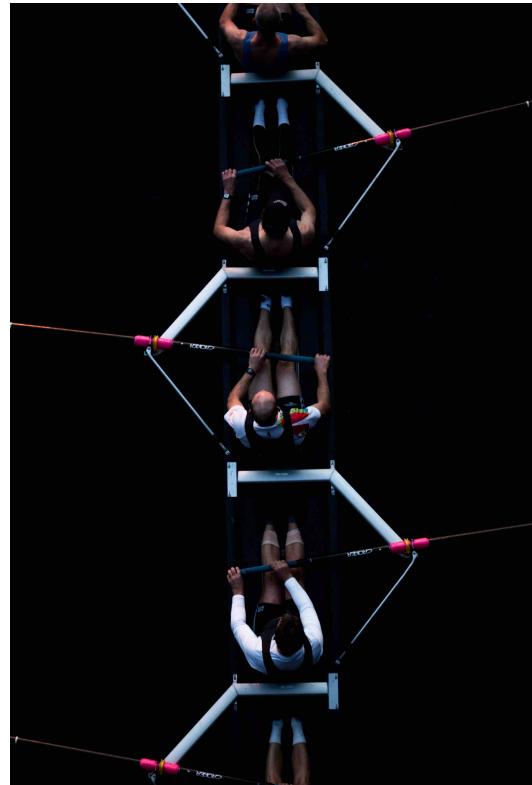


Photo by [Josh Calabrese](#) on [Unsplash](#)



TF-CSIRT

## Starting Points

Key references and other starting points

## Starting point #1 : generic



TF-CSIRT

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 : <http://www.sei.cmu.edu/legal/permission/index.cfm>

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 !**

## Starting point #3 : SIM3



SIM3 = Security Incident Management  
Maturity Model

- For (self) assessment,
- membership criteria &
- certification purposes

44 parameters in 4 categories

- O – Organisation : 10 (O-6 “intentionally blank”)
- H – Human Aspects : 7
- T – Tools : 10
- P – Processes : 17



## SIM3 Scores

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



TF-CSIRT

## ASSESSED CSIRT Maturity Example

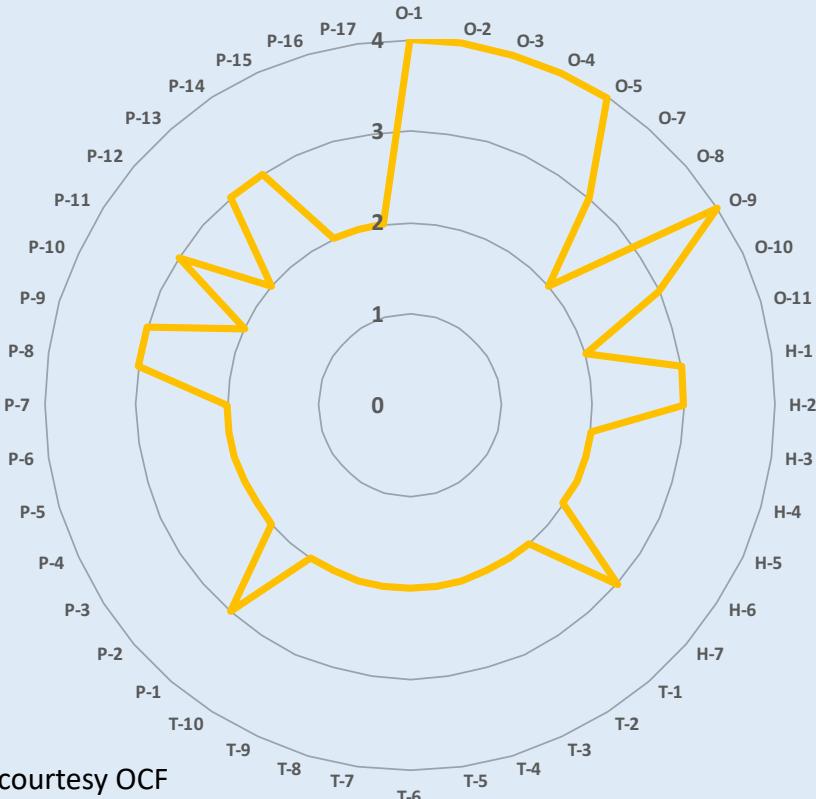


Diagram courtesy OCF



### FIRST CSIRT Services Framework

- [https://www.first.org/education/csirt\\_service-framework\\_v1.1](https://www.first.org/education/csirt_service-framework_v1.1)

### FIRST PSIRT Services Framework

- ditto for product security teams (PSIRTs) – to be published

These frameworks enumerate in depth the kind of “services” that a CSIRT or PSIRT can deliver to their constituencies (their clients)

- This is an amplification of the SIM3 parameters O-5 and O-7
- SIM3 and the service frameworks are “orthogonal”: SIM3 describes the whole range of 44 maturity parameters for a CSIRT – the service frameworks are an in depth survey of 2 of those parameters



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 the key people you need to persuade?



# Security Management Cycle



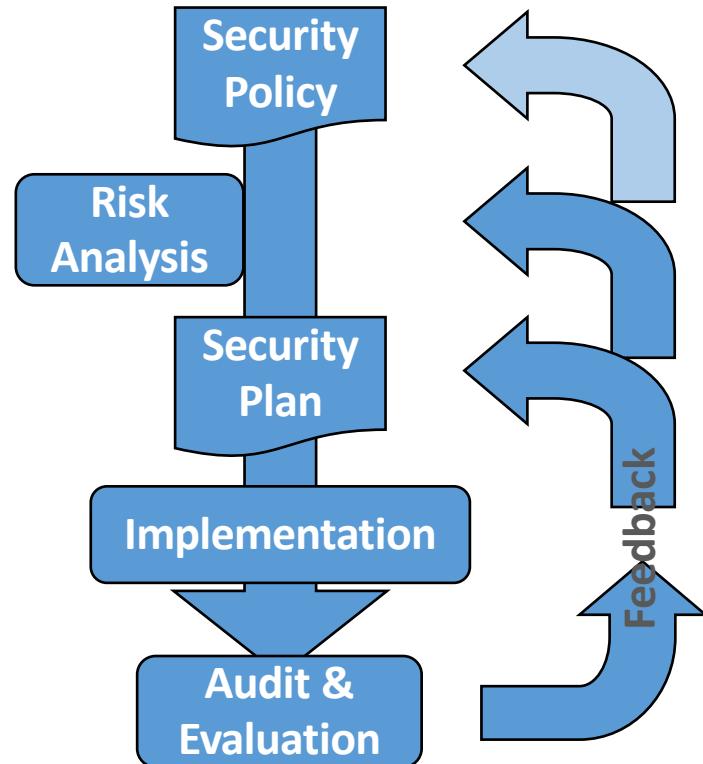
TF-CSIRT

Make sure you implement a cycle like this

- DO the feedback and ensure FOLLOW UP

CSIRT can contribute to ...

- Risk Analysis
- Security Plan
- Evaluation



# 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
- Physical security
- Risk Management
- Crisis Management
- Business continuity Management (BCM)

**End-responsible = board / CEO**



# CSIRT as spaceship

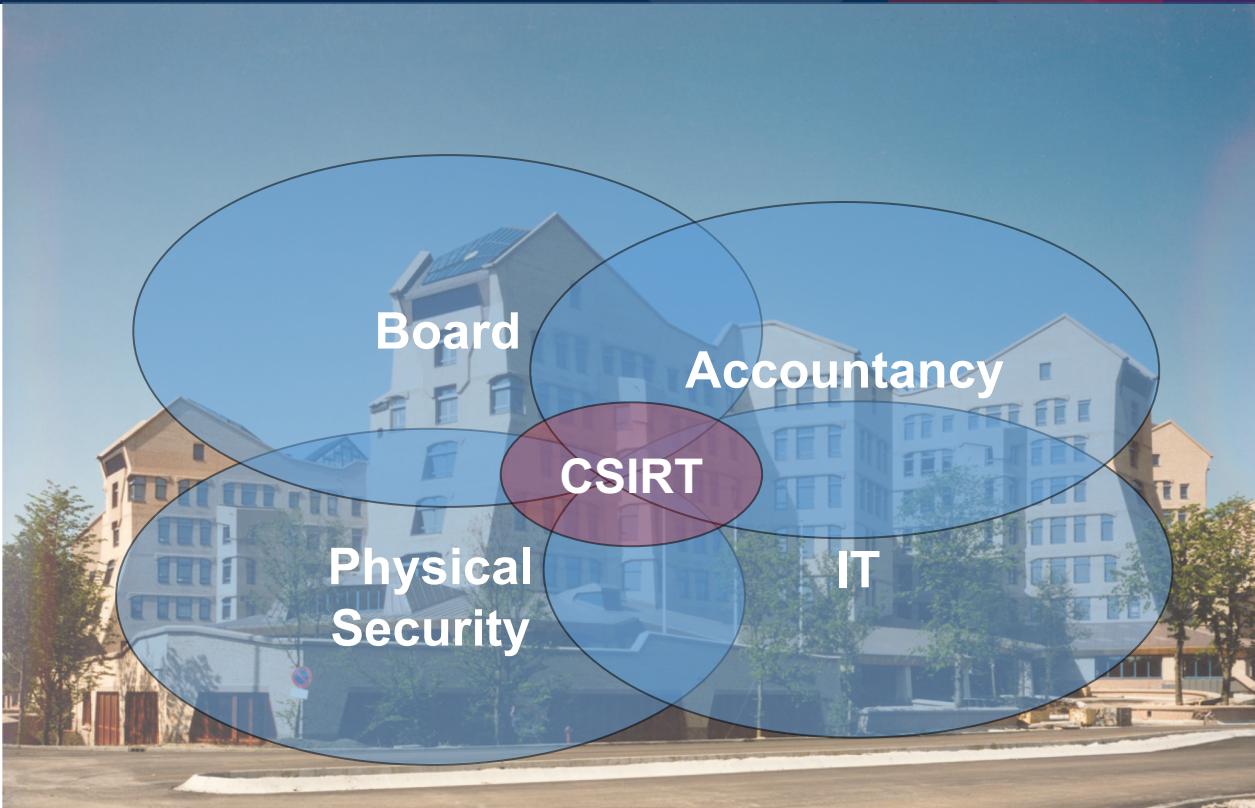
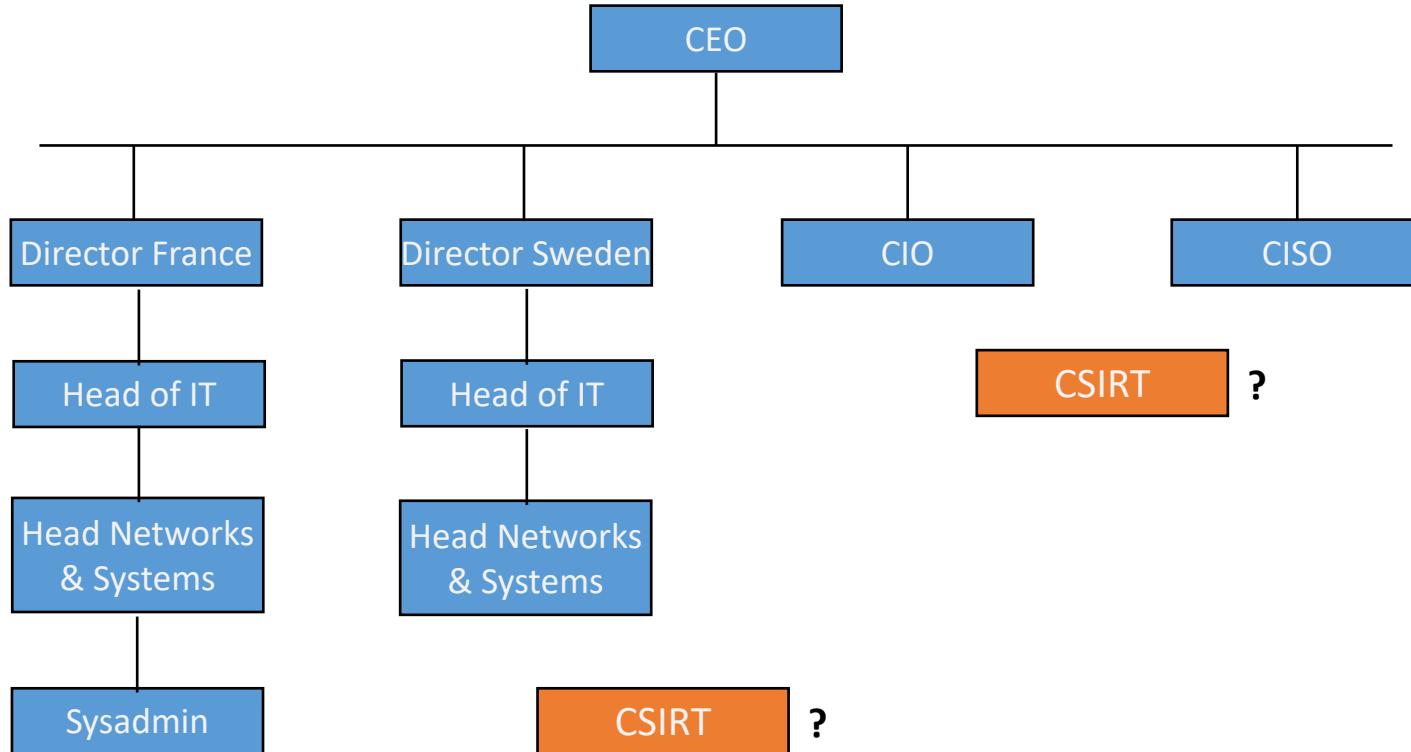


Diagram courtesy S-CURE

# Example: PariSto Bank



## Exercise (30 minutes)



TF-CSIRT

- Split into groups of 3-4 (no same org people in same group)
- In each group :
  - One member make some 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 ?
    - Responsibility : what is your team expected to do ?
    - Services : what services does your team offer to the constituency ?
    - Structure of team : central/distributed ? Experts on-call ? ( Timezones ? )
    - Place of team in organisation : where do you fit in ? Does this set-up work well ?
- Plenary wrap-up (discuss **only** highlights of group discussions)



**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





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

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 !



*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 !**

### FIRST CSIRT Services Framework

- [https://www.first.org/education/csirt\\_service-framework\\_v1.1](https://www.first.org/education/csirt_service-framework_v1.1)

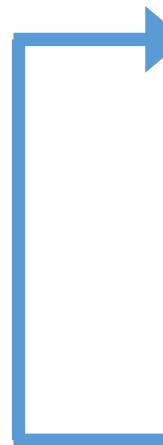
Service areas: (subdivided in services and then functions)

- Security Event Management
- Incident Management
- Cyber Threat Intelligence Management
- Vulnerability Management
- Knowledge Transfer

rfc2350 : strong advice to fill it out

- Operational factsheet of your CSIRT (services and contact data)
- Place on your team's webpages



- 
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





## PSIRTs deal with broken things

**FIRST PSIRT Maturity Document** 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/education/PSIRT-maturity-document.pdf>



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

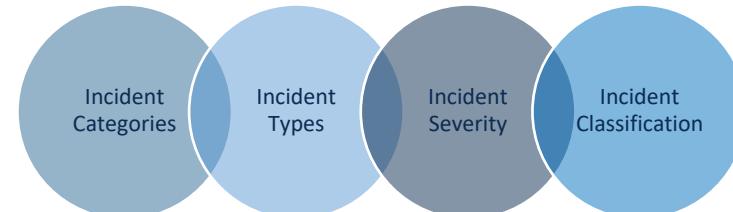
- Dependent on incident classification ?
- (Human) reaction time
- Resolution time : be **very** careful



How do you technically classify incidents ? ( = taxonomy )

- Classical taxonomies focus only on incident types.  
A good example is the popular eCSIRT.net / ENISA taxonomy :  
<https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf>
- More modern approaches also take impact/cost (and/or priority) into account.  
See e.g. <https://www.thecroforum.org/2016/06/20/concept-proposal-categorisation-methodology-for-cyber-risk/>

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



## National and International Cooperation: SIM3 O-9



TF-CSIRT





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 :  
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- Example NCSC-NL :  
<https://www.ncsc.nl/english/organisation/about-the-ncsc/operational-framework.html>



### Central (most common)

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

### Distributed

- SURFcert (serving SURFnet, Dutch NREN)
- TS-CERT and “sub-CERTs” (serving TeliaSonera ISP)

### 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 !

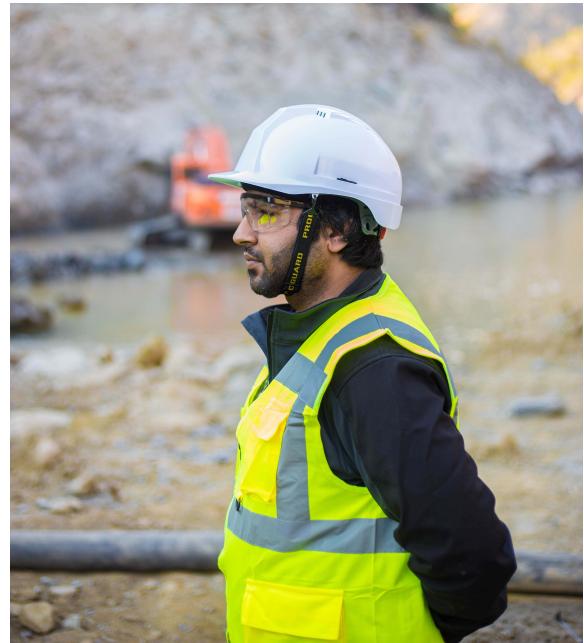


Typically a formal approach

- 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



Security policy = SIM3 parameter O-11



TF-CSIRT

## Human Factors

The main human/personnel factors to bear in mind

## Exercise (20 minutes)



TF-CSIRT

- Split into same groups of 3-4 as before
- In each group :
  - One member make some 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 ?
    - Do you have access to training / training budget for your staff ?
    - 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** highlights of group discussions)



**The human factor is the prime factor in the success of any CSIRT** - Without a good, trustworthy team ... nothing goes

### **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>

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

“Who polices the police” applies to CSIRTs too



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



### 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, ...

### Need other resources ?

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

# Personal development → team development



## Personal development plan

- 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)



Internal training = SIM3 parameter H-4  
Technical training = SIM3 parameter H-5  
Communication tr. = SIM3 parameter H-6



## Internal Training

Internal Tools

Team Building

Local Processes

## Technical Training

TRANSITS

FIRST

ENISA

APNIC

## Communications Training

General Communications

Presentation skills

Speaking to press

Dealing with police



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 for a
  - 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 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 Immanuel Kant or your trainers here – nor your colleague who has done this work for 15 years



- NCSC-cyber security assessments :

<https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands>

- Various reports: we all suffer from security incidents

- Annual cost of global cybercrime

- Symantec: \$110 billion in 2012

- McAfee: \$ 600 billion in 2017 <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf>

- 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/>

## Reading List (1)



TF-CSIRT

- SIM3: <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>.
- RFC2350: <https://www.ietf.org/rfc/rfc2350.txt>.
- ENISA CSIRT Maturity: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey>.
- Trusted Introducer Accreditation Package: <https://www.trusted-introducer.org/invitation-package.pdf>
- Permission to Use CERT: <https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/>.
- CSIRT Handbook:  
[https://resources.sei.cmu.edu/asset\\_files/Handbook/2003\\_002\\_001\\_14102.pdf](https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf).
- Software Engineering Institute CSIRT Services:  
[https://resources.sei.cmu.edu/asset\\_files/WhitePaper/2002\\_019\\_001\\_53048.pdf](https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf).

## Reading List (2)



TF-CSIRT

- FIRST CSIRT Services Framework : [https://www.first.org/education/csirt\\_service-framework\\_v1.1](https://www.first.org/education/csirt_service-framework_v1.1).
- ENISA Reference Incident Classification Taxonomy:  
<https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>.



**TF-CSIRT**

**Thank you !  
Any Questions ?**

**Authors: Serge Droz, Jaap van Ginkel & Don Stikvoort**

Version: 7.2

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