National and sectorial CSIRTs: implementation and cooperation models

Otmar Lendl <lendl@cert.at>

Quick Intro

- Mag. Otmar Lendl
  - Uni Salzburg, EUnet, KPNQwest, nic.at
  - Teamleader CERT.at since 2008
  - Currently acting as chair of the CSIRTs Network

Content

- Roles
  - National CERT (pre-NIS)
  - National CSIRT (NIS)
  - Sectoral CSIRT (NIS)
- Collaboration
  - People
  - Systems
- Setups

Terminology

- CERT vs. CSIRT
  - Computer (security incident | emergency) response team
  - CERT™ by CMU -> NIS-D is using CSIRT
  - Synonyms

- (see also https://cert.at/services/blog/20180731155524-2252_en.html)

CERT/CSIRT Designation

- The right to use the CERT trademark (granted by CMU/CERT-CC)
- **Membership** in FIRST (the global association of CSIRTs)
- **Registration**/**Accreditation**/**Certification** in the Trusted Introducer Directory
- Formal **designation** as CSIRT by a national authority according to the national implementation of the NIS-D (Article 9)
- Listed on the ENISA CSIRT map
- Membership in the CSIRTs Network
- Membership in regional CERT associations (e.g. German CERT-Verbund, EGC)
- Reputation as a valuable peer built over years of collaboration with other CSIRTs

Types of CERT/CSIRTs

- Lots of variation

- Small team in an academic setting
- Big team in a National Cyber Security Center

- CSIRT Taxonomy?

Criteria (1)

- Protect what?
  - Computer Infrastructure: - CSIRT
  - Product Security: - PSIRT
- Role of the CSIRT?
  - Advisory role only
  - Reporting requirements exist
  - CSIRT can order countermeasures

Criteria (2)

- Definition of the Constituency?
  - Geographic boundary: city, state, country, region, global
  - Specific sector: government, military, academics, sectors of the critical infrastructure or operators of essential services, ...
  - Specific Company: e.g. Siemens AG

Criteria (3)

- Relation to Constituency?
  - Part of same organization: e.g. siemens-cert
  - CSIRT services are part of some other contract: NREN-CERTs, ISP abuse teams, some GovCERTs, financed by chamber of commerce (or similar) ...
  - Outsourced/Contracted CSIRT service
  - No contractual relationship: national CERTs

Pre NIS National CERT

- ENISA (2009) National CERT Informal definition:
  - A CERT that acts as national point of contact (PoC) for information sharing (like incident reports, vulnerability information and other) with other national CERTs in the EU Member States and worldwide. National CERTs can be considered as "CERT of last resort", which is just another definition of a unique national PoC with a coordinating role. In a lot of cases a national CERT also acts as governmental CERT. Definitions may vary across the EU Member States!

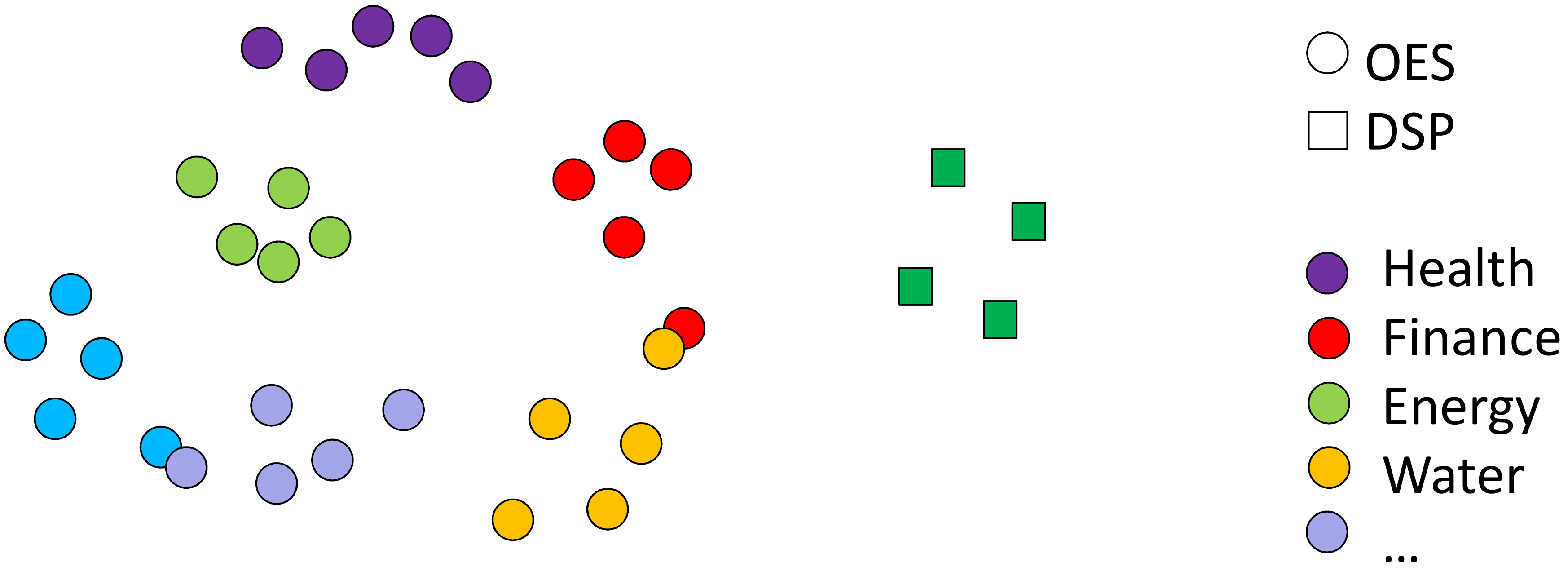
National CERT

- Principle of Subsidiarity: If there is another CERT more closely associated with the affected system, then that team will take care of the incident. A national CERT is the "default" or "fallback" CERT.
- The "national CERT" will act as information hub: both inside the country as well as a point of contact for the country for foreign CERTs.
- Its role is usually rather hands-off: it will provide guidance, publish warnings, incident notification and will not generally provide on-site remediation help.

NIS-D CSIRTs

- Article 9:
  1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.
- **Only covers OES/DSS**

Graphically



○ OES

□ DSP

● Health

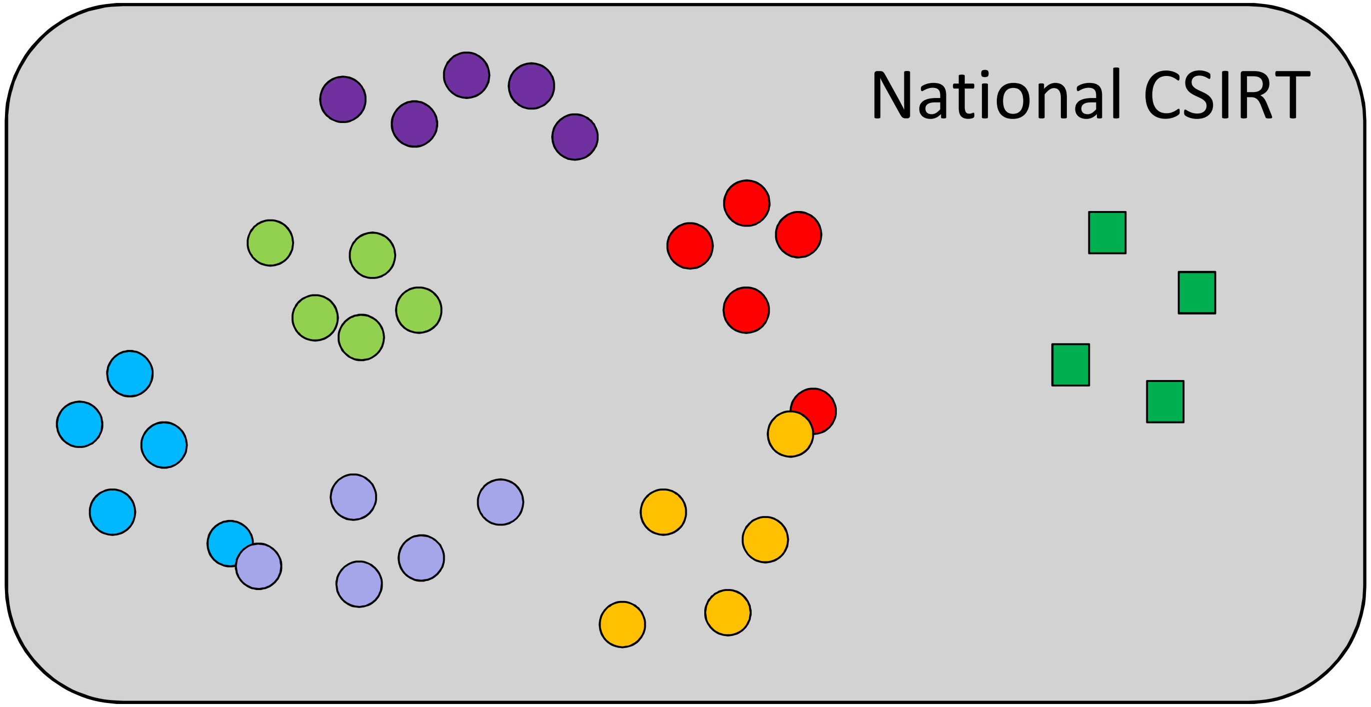
● Finance

● Energy

● Water

● …

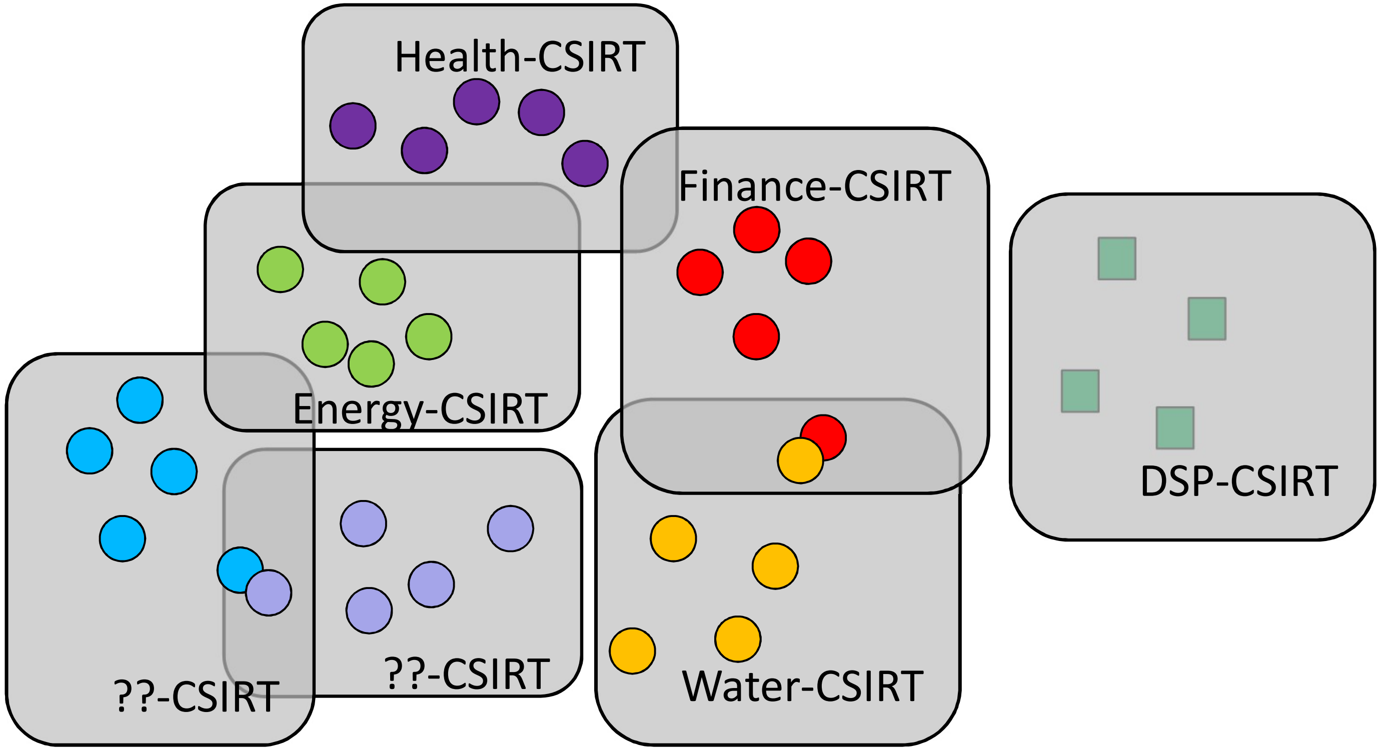
Centralized



○ OES
□ DSP

● Health
● Finance
● Energy
● Water
● …

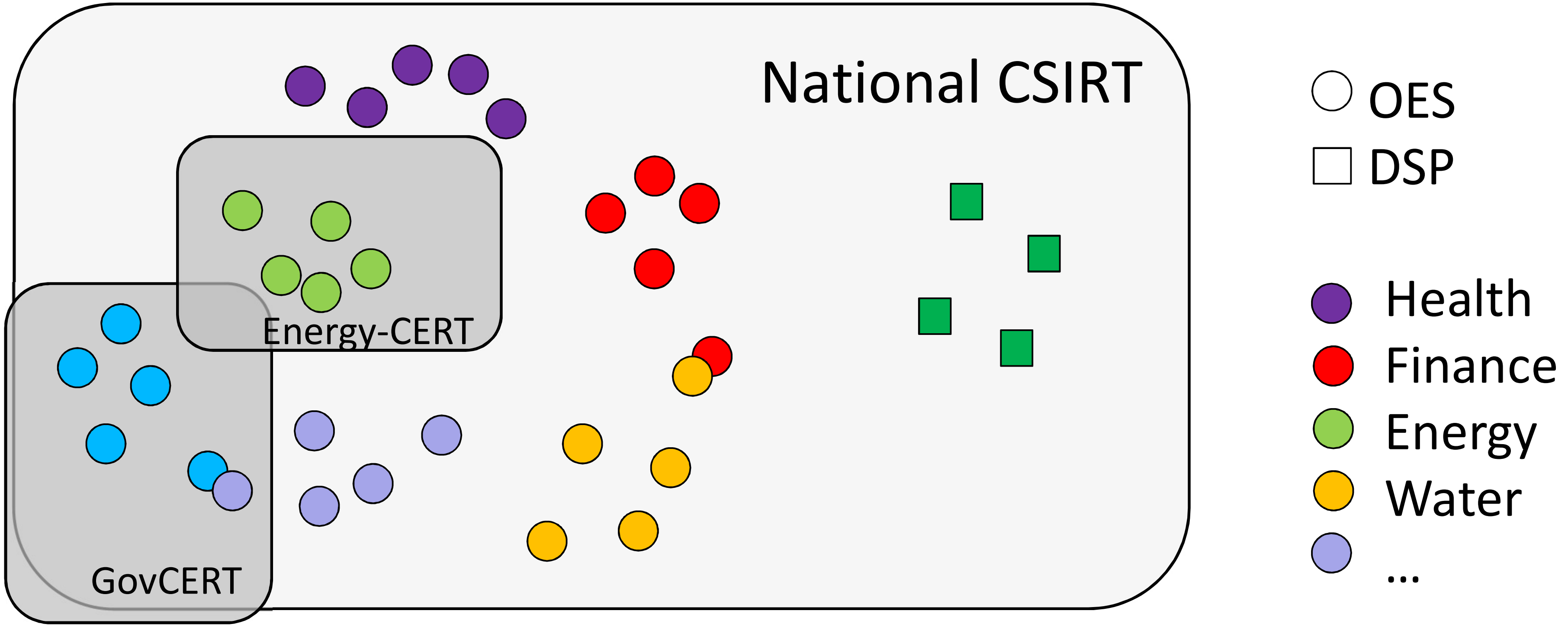
Pure Sectoral



○ OES
□ DSP

● Health
● Finance
● Energy
● Water
● …

Mixed (e.g. Austria)



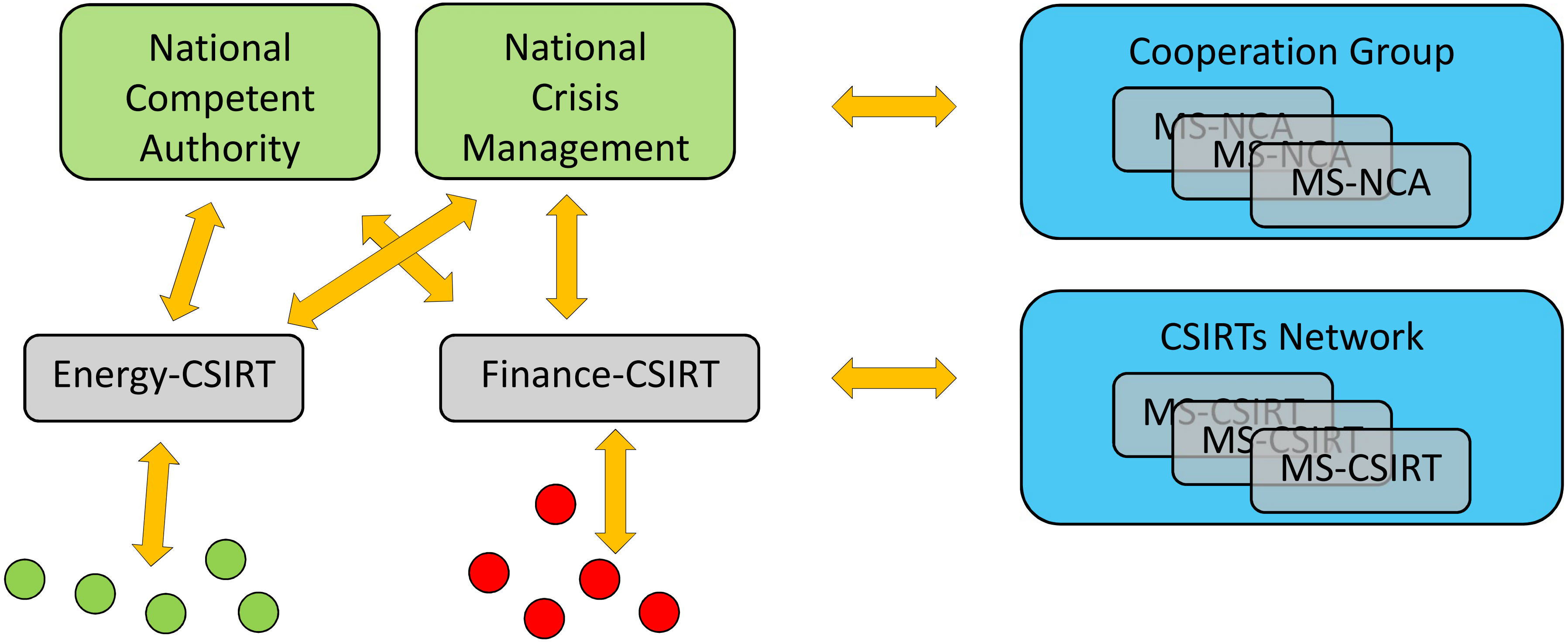
Pro/Con

- Centralized
  - Bundling of resources
  - Less friction / coordination effort
  - Good for small countries
- Sectoral
  - Industry chooses their own CSIRT -> Trust
  - Chance to specialize on domain knowledge
- In AT: Energy and National CERT in same organisation

Don‘t forget the NCA

- Almost the same applies to „national competent authorities“
- We see all kinds of models in the EU
  - 1 NCA, sectoral CSIRTs (AT)
  - Sectoral NCA, one national CSIRT (UK, FI)
  - 1 NCA, 1 CSIRT (DE)

CSIRT Communication



National Competent Authority

National Crisis Management

Energy-CSIRT

Finance-CSIRT

Cooperation Group

MS-NCA

MS-NCA

MS-NCA

CSIRTs Network

MS-CSIRT

MS-CSIRT

MS-CSIRT

2018/11/27

CSIRT Sharing levels

- Constituent
- Sectoral trust groups (industry, government)
- National CERT Forum
- National NIS coordination (IKDOK/OpKoord)
- Closed national Mailinglists (NOG, Discuss, …)
- Regional CERT Forums (EGC, CECSP)
- CSIRTs Network
- TF-CSIRT / FIRST / (various Mailinglists / Forums)
- Public (Blog, Warning)

Collaboration needs

- Who to talk to?
  - Directory
- What to share?
  - What can the use?
- Can we share?
  - Legal framework
  - TLP
  - Crypto

- Do we want to share?
  - Trust
- Can we make use of incoming data?
  - TLP:RED == TLP:Nothing-to-do
  - Capabilities

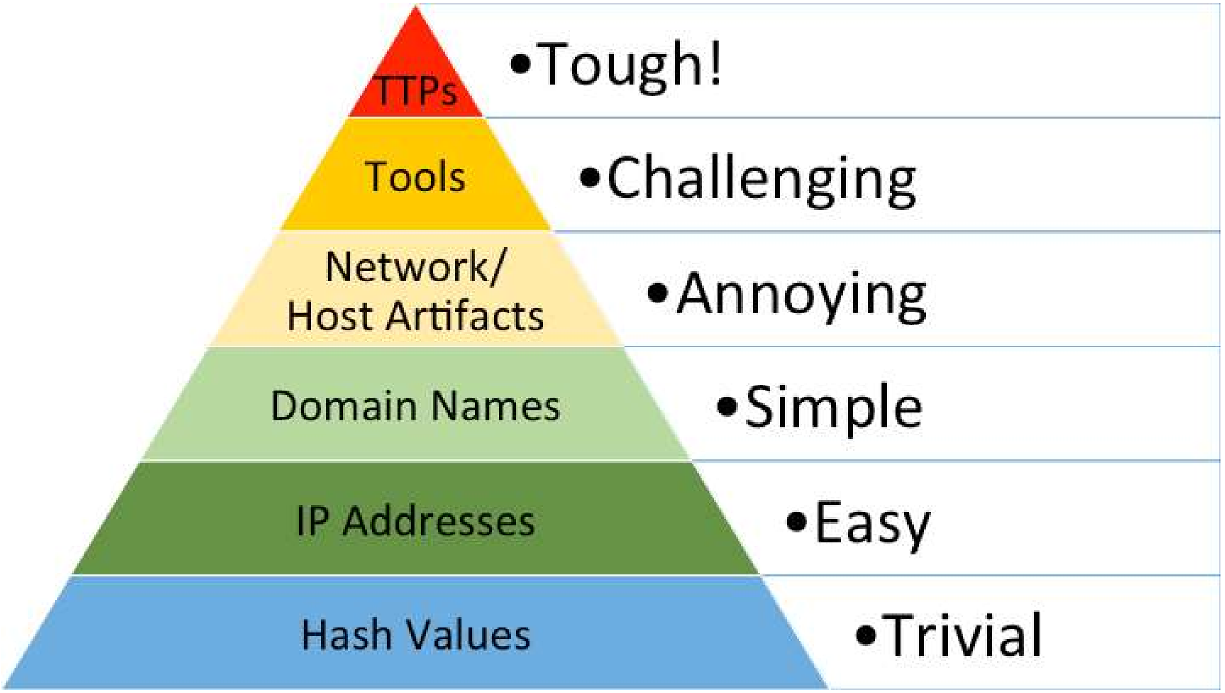
The People Side

- Our experience:
  - Daily work is less technical than expected
  - Lots of it is playing matchmaker: people + people + information
  - People >> teams
- Thus:
  - When designing cooperation: think about people
  - They must be comfortable with the collaboration

Technology

- Human – Human is manageable
- Machine – Machine:
  - Local Automation is the key

The Pyramid of Pain



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Challenge

- For the constituency:
  - Can they process Threat Intelligence Information and action on them?
  - As far up the pyramide as possible
  - Preferrably automatic (STIX2, MISP)
- For the CSIRTs
  - Collect and process CTI
  - Share amoungst peers (automatically!)
  - Provide this data to the constituency

Questions?

- http://www.cert.at/
- Otmar Lendl <lendl@cert.at>