# CERT coaching in (own) practice – case studies and roads into future

Przemek Jaroszewski
CERT Polska/NASK

**Coaching** is a teaching or training process in which an individual gets support while learning to achieve a specific personal or professional result or goal. (Wikipedia)

- in sports
- in professional carreer
- in personal development
- and many more…

# S.M.A.R.T. Goals are smart

Specific
Measurable
Acceptable
Realistic
Time-based

(Blanchard, Zigarmi, & Zigarmi, 1985)

# CLOSER (2007-2009)

- CERT Polska, CEENET, SurfNET
- 100% funded by NATO
- Help in setting up CERTs in CEENET NRENs
  - Focus:  AZ, AM, GE, MD, UK, UZ
  - Other: MK, BG, BY, KZ, KG, Kosovo
- Assistance in the first phase of their existence
- Operational assistance
  - Forward of relevant incident data
  - Assistance in handling
- Goals
  - At least two become full FIRST members by 2009
  - At least four become TI Accredited by 2009

# CLOSER - observations

- NATO subsidies were consumed mostly for hardware purchases (CERT = "CERT equipment" )
- NRENs in Central Asia tend to be largely dependent on politics
- CERT operations depended on individuals' passion
- Trained personnel often left to work for commercial companies or government


Source: www.cert.md

# Moldova

- MD-CERT is run mostly as hobby of network administrators in RENAM
- CERT is "alive" (TI Listed), but hardly active – last website update in 2010

# Azerbaijan

- CERT AzEduNET effectively ceased to exist
- Other academic CERT: AZ-CERT formed in Azerbaijan National Academy of Science in 2011
  - TI Accredited in May, 2011
- Government CERT: CERT.GOV.AZ formed in Special Communication and Information Security Department in 2012
  - Full FIRST member since July, 2011

# Georgia

- CERT-GEORGIA in GRENA played an important role in coordination during 2008 crisis, now effectively inactive
  - TI Accredited in 2011, suspended in 2012
- CERT.GOV.GE established in 2011 in Data Exchange Agency
  - TI Accredited in 2012, likely to apply for full FIRST membership

# CLOSER – Lessons learned

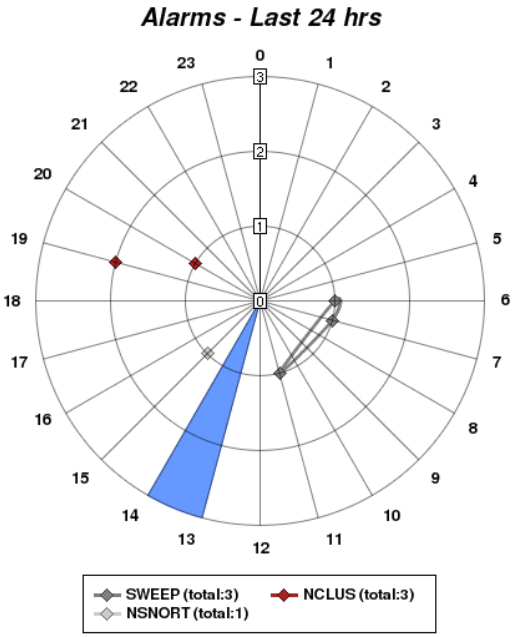
- Finantial incentives are not the best incentives
- Motivation and commitment are essential (agreement on goals!)
- Building of trust in own capabilities
  - Incident data feeds
  - Support

# Too few incidents… or too many?

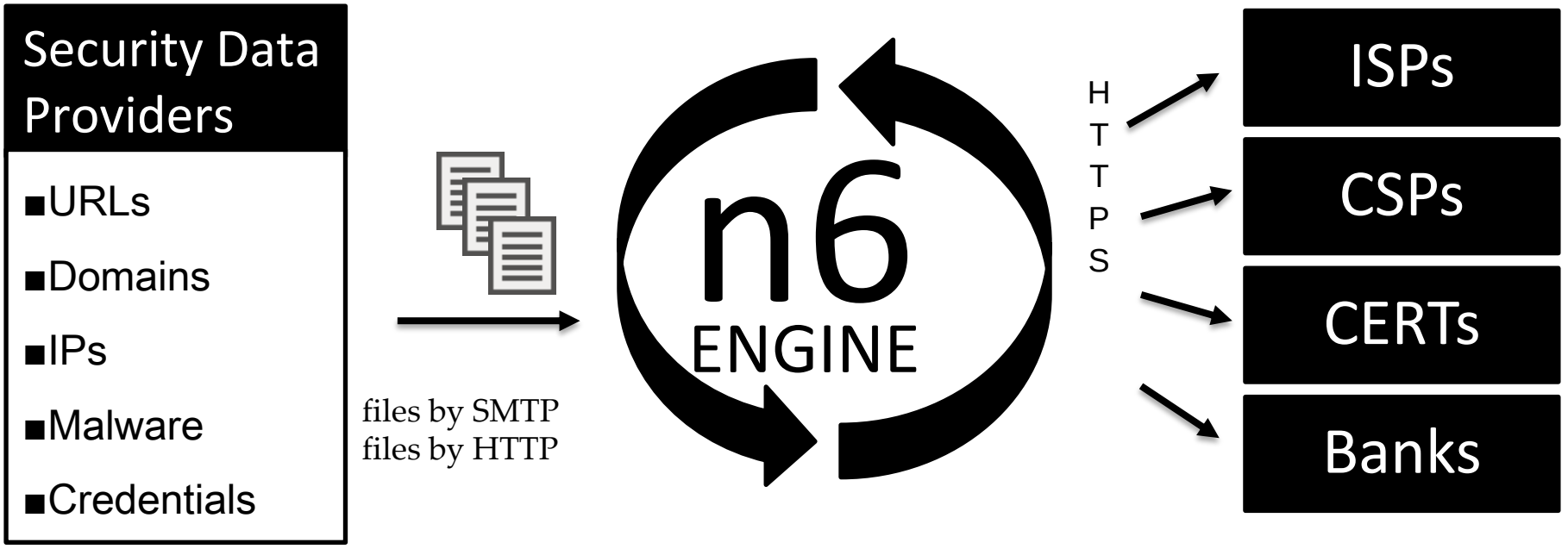
- New teams complained about lack of incident data
- Refer to ENISA document *Proactive detection of network security incidents* (2011)
- Help select appropriate sources
- Use own detection systems
- Avoid data floods

# Case study: ARAKIS

- Early warning system developed in CERT Polska in 2006 for CERT.GOV.PL
- CERT.GOV.PL gets valuable insight in security of government networks
- Attacks detected from countries participating in CLOSER forwarded to appropriatr CERTs
  - Not equally good for everyone

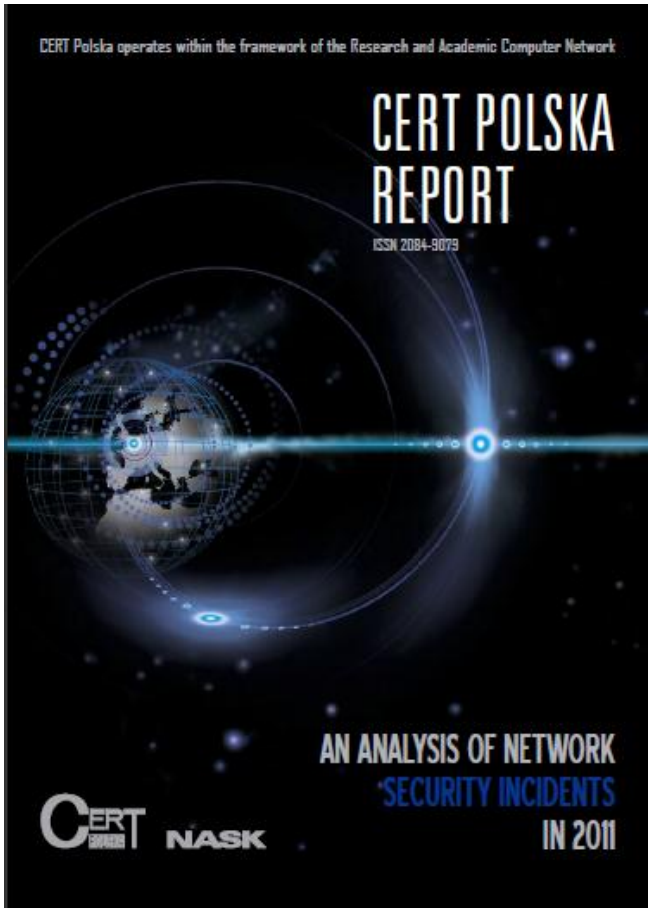


# Case study: n6



# Measurable goals

- AS reputation
- Number of infections per IP
- Number of spam messages per IP
- Use existing ratings or create metrics in own systems



# Gamification?

You have earned a trophy.
**Clean network**

- It's fun to achieve goals ☺
- Such badges may have a commercial value for ISPs

# Conclusions

- Learn the real motivations of the coachee and plan your actions and expectations accordingly
- Agree on achievable, measurable and time-based goals
- Don’t be afraid to miss some of the goals
- Try to have fun!

# Thank you!

## Questions?

**przemek@cert.pl**