Applying HPC infrastructure for advanced cybersecurity services for improving protection in the public sector

Mikołaj Dobski, Gerard Frankowski, Norbert Meyer, Maciej Miłostan, Marek Pawłowski, Błażej Pelichowski

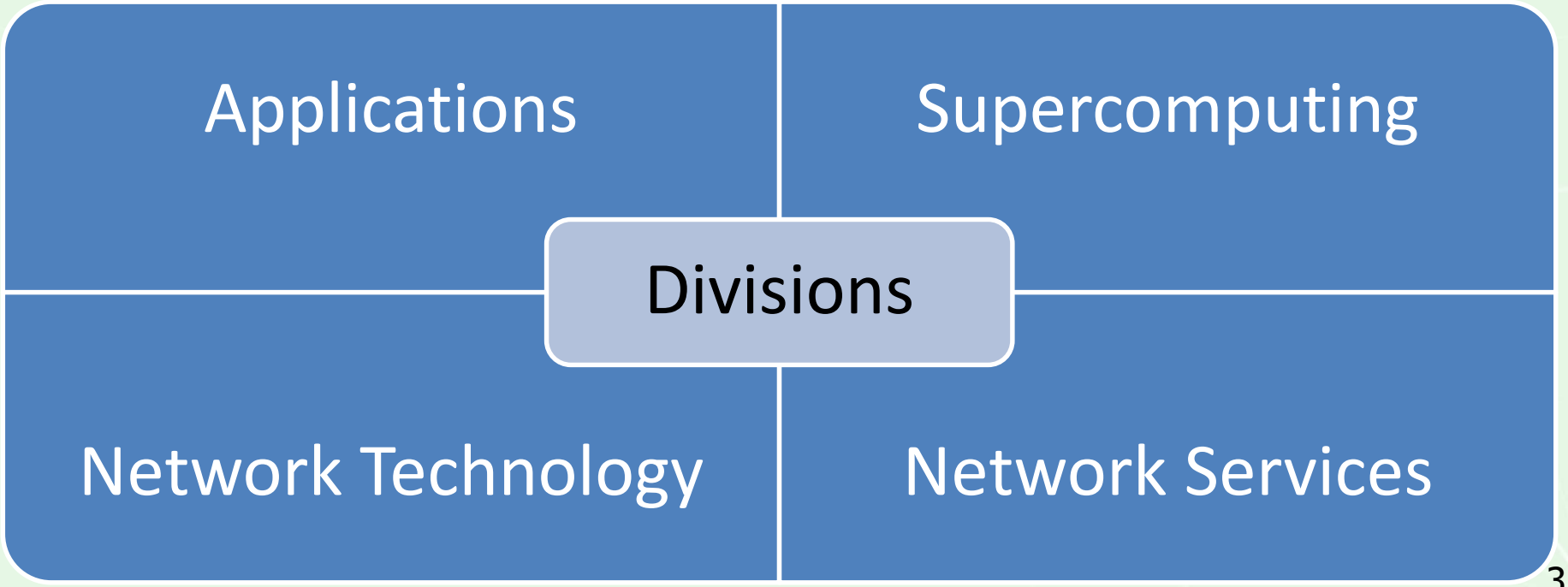
Cracow Grid Workshop 2016 – 25.10.2016

Welcome!

Where are we from?

- Operator of PIONIER (Polish NREN) an
  POZMAN networks
- European and Polish R&D Projects
- R&D together with science, industry,
  finance, administration, government, ..
- Main areas of interest
  - New generation networks (NGN)
  - New data processing architectures
  - Internet of Things services
  - Security of systems and networks

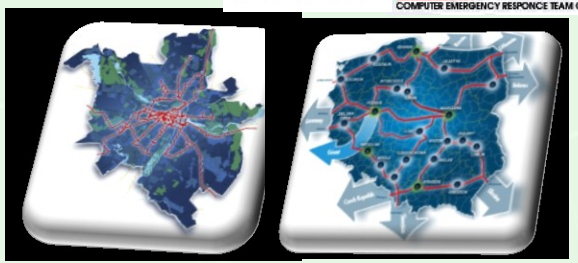
PSNC technical divisions



PSNC Cybersecurity Department

What we do about cybersecurity in PSNC?

- Since 1996 (formerly PSNC Security Team)
- Currently 10 security specialists
- Main areas of activity:
  - Securing PSNC, PIONIER, POZMAN infrastructure
  - Security tasks in R&D projects
  - Knowledge transfer
  - Vulnerability and security research
  - External services



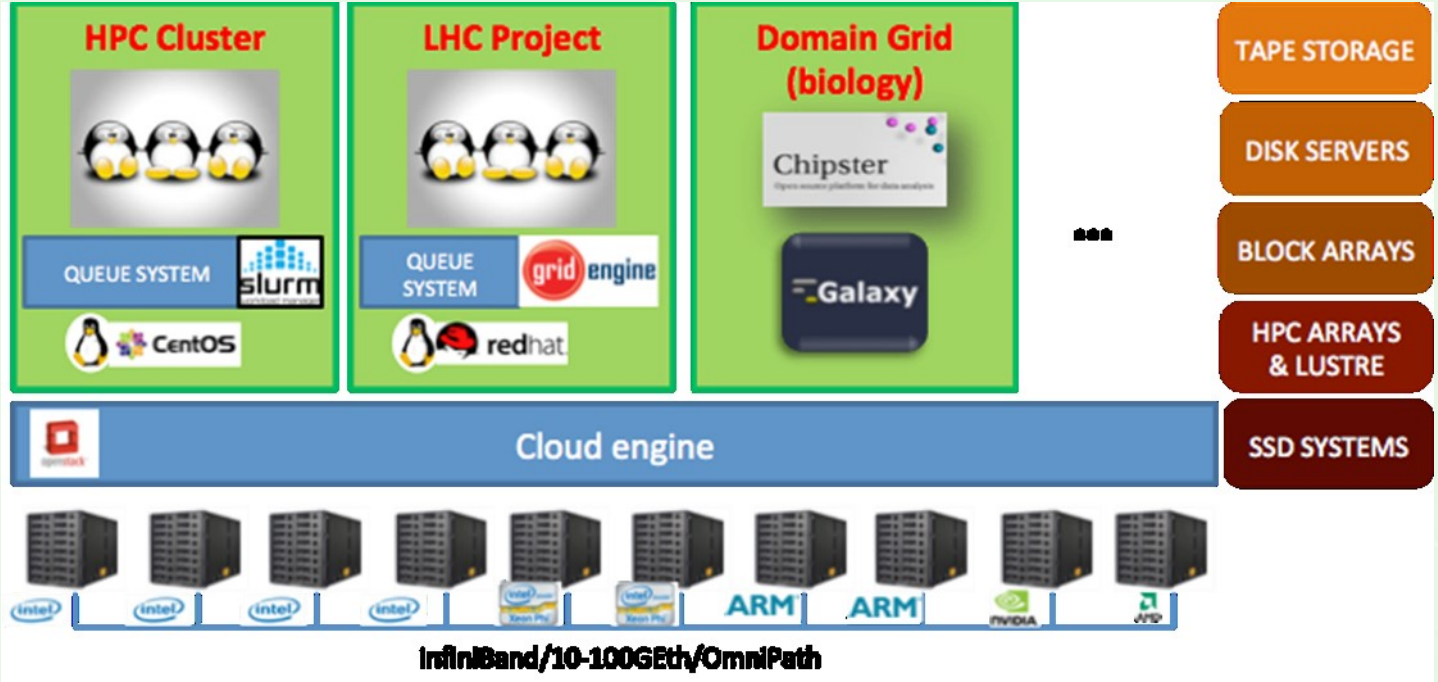
„Eagle” system @PSNC

- 1.4 Pflops
- 80th @ TOP500 on Nov 2015
- 33k cores / E5-2697v3
- 301 TB RAM
- Infiniband FDR
- DLC-cooled,
- 0,55 MWatts - PUE: 1,04

PSNC - HUAWEI INNOVATION CENTER

WHERE TECH MEETS SCIENCE

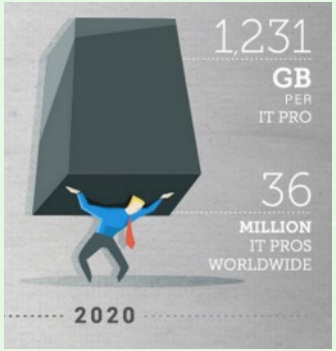
Pairing HPC & Cloud computing models



Data management challenges

DATA STORAGE:

- growing volume: PetaBytes
- pressure for performance: GB/s, IOPS
- long-term storage: costs, consistency, durability



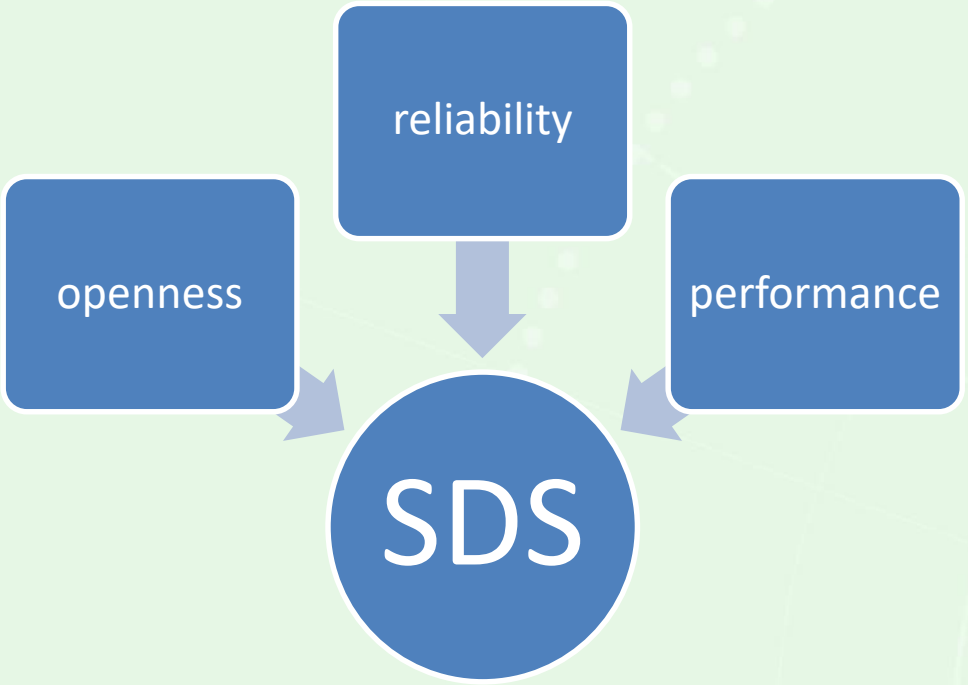
DATA PROCESSING:

- cloud: serving fast & reliable data volumes to VMs
- HPC: efficient storage: job in/out/scratch, checkpoints
- real-time data analytics within storage

Big Data processing in-storage

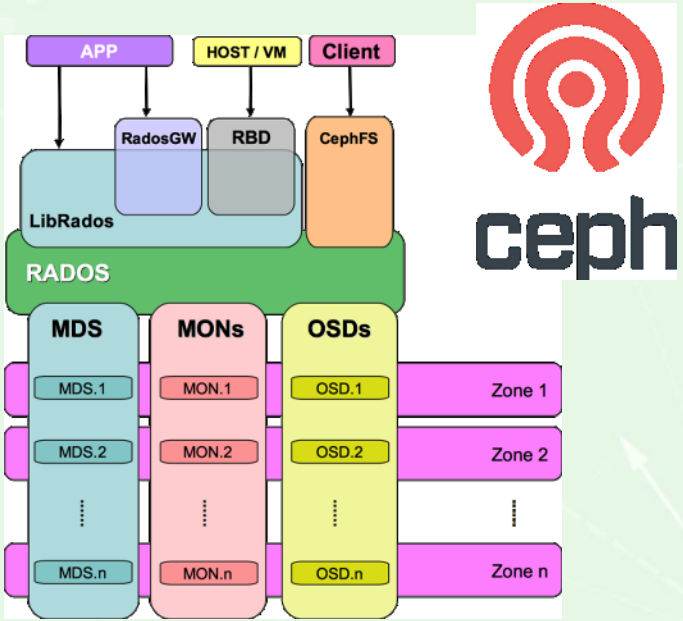
„Miracle solution”

Software Defined Storage



CEPH Storage

- FULL DECETRALISATION
- NO SPOF + NO BOTTLENECK
- SCALABILITY
- LOAD-BALANCING,
- FAULT-TOLERANCE
- INTEGRATION / PROTOCOLS:
  - Object (RADOS, S3, Swift)
  - Block: RBD:
  - Filesystem



Software defined storage

Hadoop @OpenStack Swift @CEPH @HW

Hadoop oD

OpenStack Swift

Ceph

Lots of resources…

- Why do we need all this?

The Polish Ministry of Foreign Affairs SIEM processes daily 20GB of data
Public procurement docments

The HP cybersecurity center receives daily between 10^11 and 10^12 events that may be related with cyberthreats, and is only able to process up to 3*10^9 of them
S. Bhatt, P. K. Manadhata, L. Zomlot, "The Operational Role of Security Information and Event Management Systems"

Daily stream of cybersecurity events

Every day there are published:
2000 technological blog articles
500 000 articles in all media
30 R&D papers
25 vulerability reports
concerning cybersecurity

Martin Borrett – IBM Distinguished Engineer and CTO
IBM Security Europe
Cybersec.eu conference, September 2016, Kraków

Entire US political system 'und
Russian hacking, experts warn

Meanwhile, some US commentators on cybersecurity issues h
attacks are not a surprise but appear to be a new spin on an old

"Internet of Things" security is hilariously broken and getting worse

Shodan search engine is only the latest reminder of why we need to fix IoT security.

by J.M. Porup (UK) - Jan 23, 2016 4:30pm CET

Share Tweet Email 137

ch engine for the Internet of Things (IoT), recently launched a new section that lets
wse vulnerable webcams.

es images of marijuana plantations, back rooms of banks, children, kitchens, living
, front gardens, back gardens, ski slopes, swimming pools, colleges and schools,
d cash register cameras in retail stores, according to Dan Tentler, a security
has spent several years investigating webcam security.

place," he told Ars Technica UK. "Practically everything you can think of."

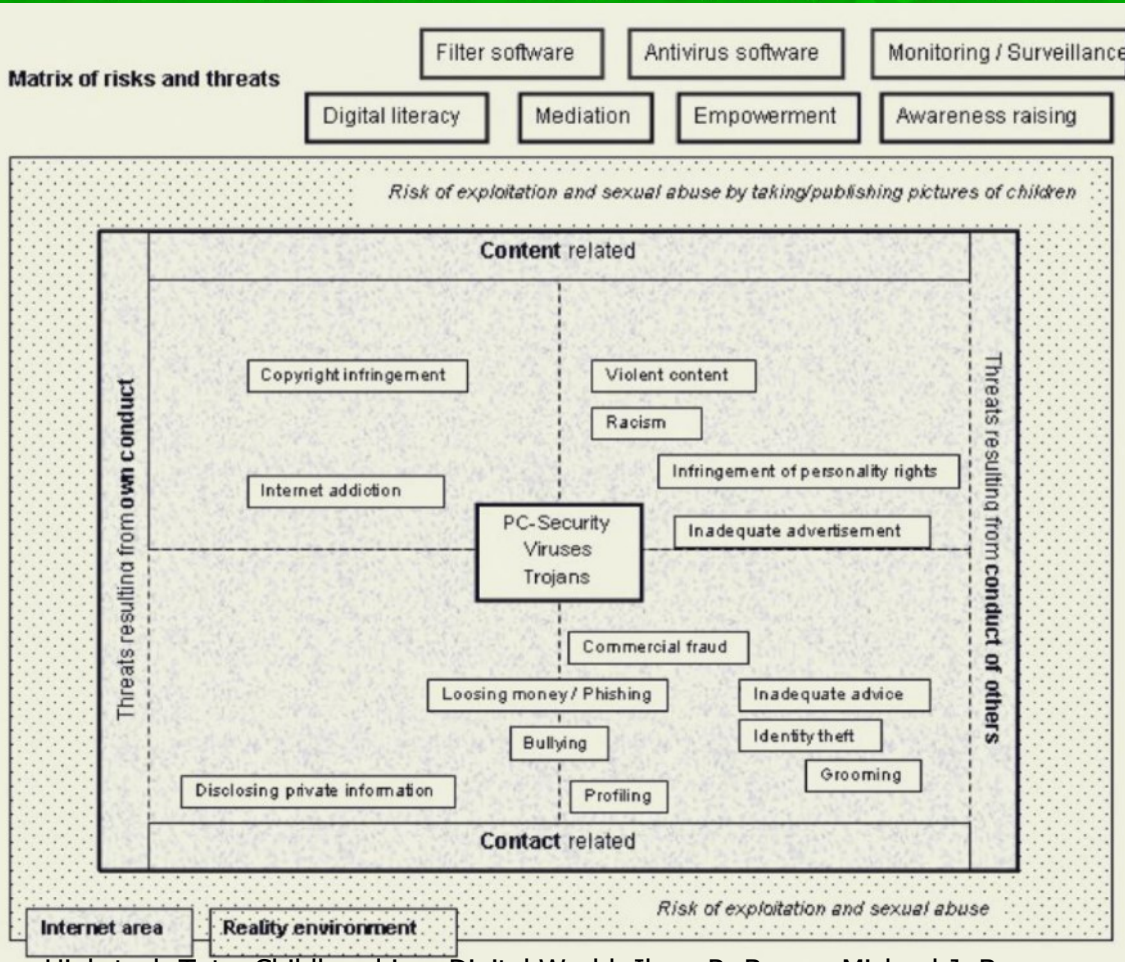
search and turned up some alarming results:

Sources: www.samorzad.lex.pl, www.polskieradio.pl, www.dzienniklodzki.pl

Attacks and threats

People and infrastructure protection

- Online threats to people:
  - 3 Cs (content, contact, conduct)
- Infrastructure attack
  - DoS, DDoS, DRDoS
  - Hacked systems
  - Malicious code injection



High-tech Tots: Childhood in a Digital World, Ilene R. Berson,Michael J. Berso

Who is being targeted?

We want the Public Sector to go online.

IT End-users:

- sys-admins
- software developers
- management
- HR
- clerks
- visitors
- … ?

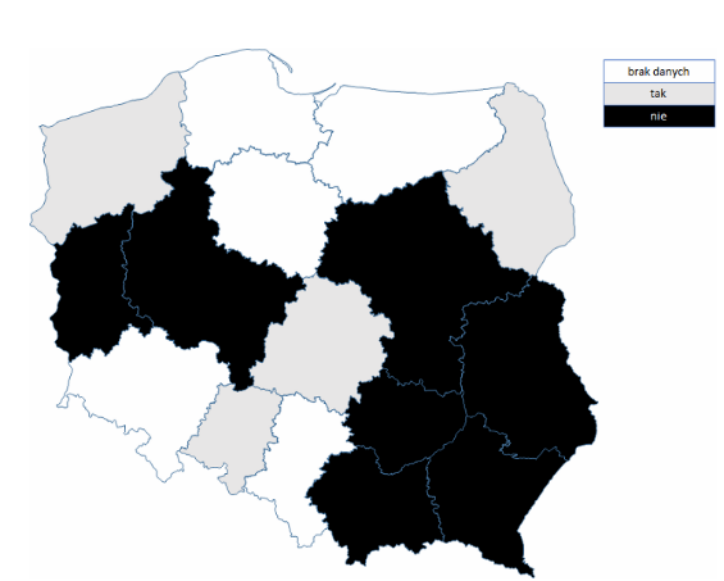
In 48 out of 50 cases persons who found a planted smartphone, run applications installed on it

Paweł Wojciechowski, Symantec

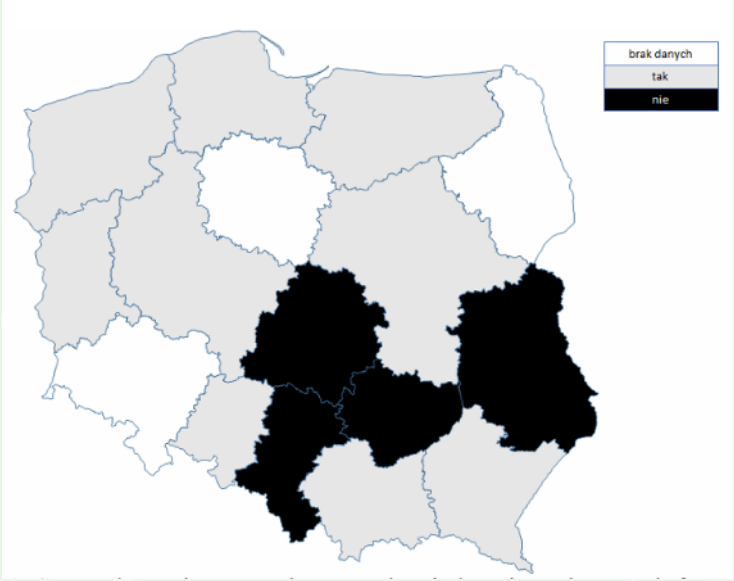
Specific factors escalating cybersecurity problems in the public sector

- Employment problems
  - Lower wages
  - ICT Department is often also Helpdesk
- Procedural issues
  - Long proceeding of standards and regulations
- Problems with investing in ICT infrastructure
  - Long public procurement procedures
  - Difficulties in preserving homogeneity of the IT infrastructure

Public sector's administration is getting more secure, but there is still much work to be done



Information Security Management System (ISMS) deployment status in voivodeship offices.



Information Security Management System (ISMS) deployment status in Marshal offices.

No data
Yes
No

Source: *Cybersecurity of Public administration in Poland. Selected topics (April 2016)*

How to prevent security incidents?

Basic attacks countermeasures

Security systems

Human awareness

Automated patches

Procedures & policies

Project Management

But we need more!

Advanced systems able to detect unknown threats

SECOR Project

SECOR – **Se**nsor Data **Cor**relation Engine for Attack Detection and Support of the Decision Process

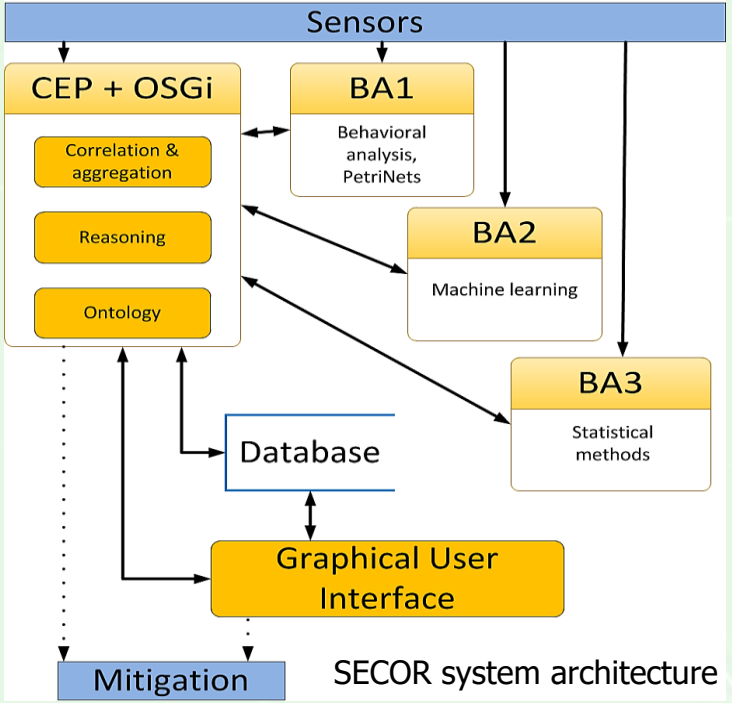
- Applied Research Programme (PBS) of the National Centre for the Research and Development (NCBiR)
- The Consortium:
  - Military Communication Institute (WIŁ)
  - Poznań Supercomputing and Networking Center
  - ITTI Sp. z o.o.

SECOR (continued)

Blocks of Analysis (BAs)

- BA1: behavioral analysis, Petri nets
- BA2: machine learning
  - Neural networks
  - Graph clustering algorithms
  - Machine learning
- BA3: statistical methods

- This project proves that the **correlation** of security alerts obtained with different methods actually works



SECOR system architecture

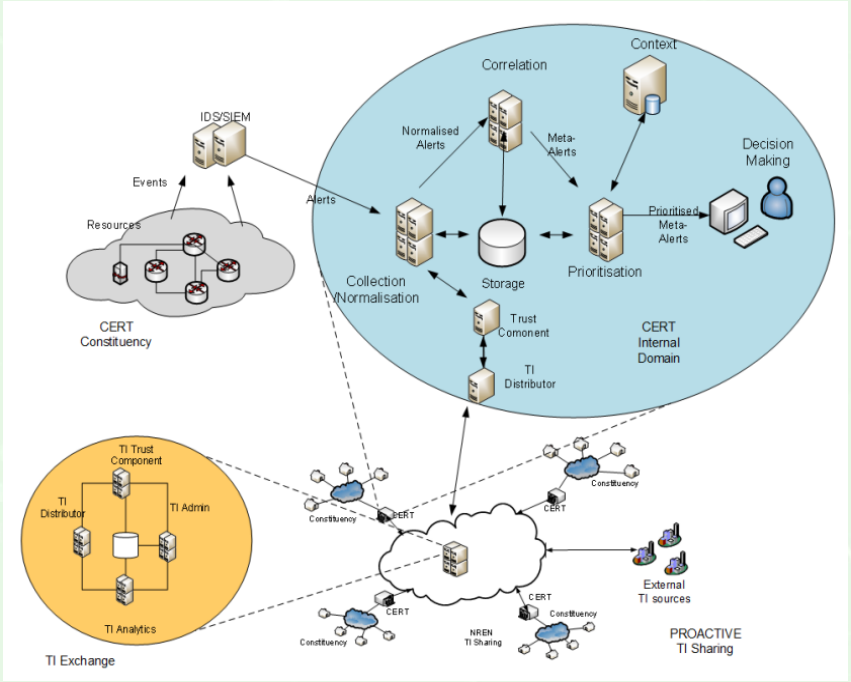
Protective H2020

Proactive Risk Management through Improved Situational Awareness

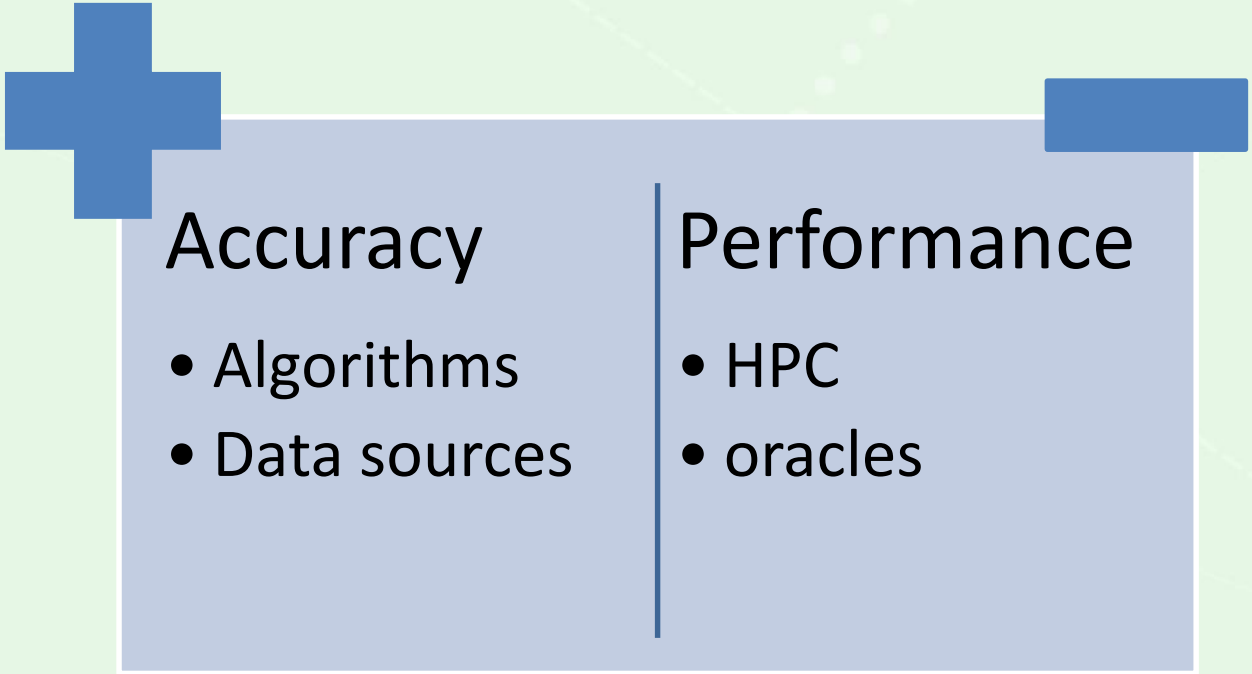
Increasing threat awareness

Prioritizing security alerts

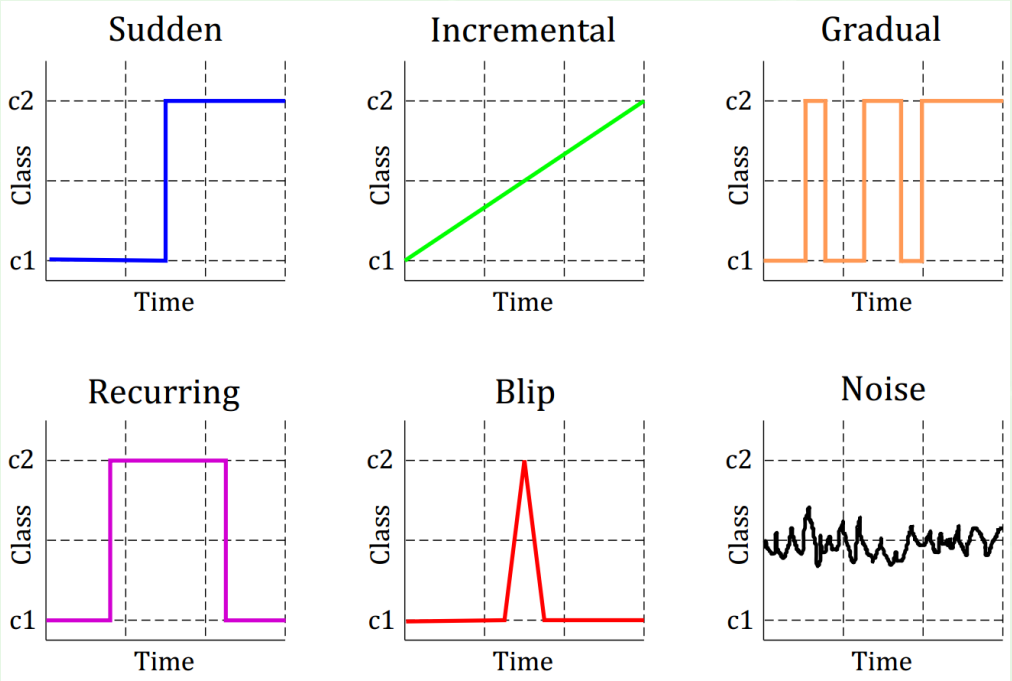
Sharing Threat Intelligence



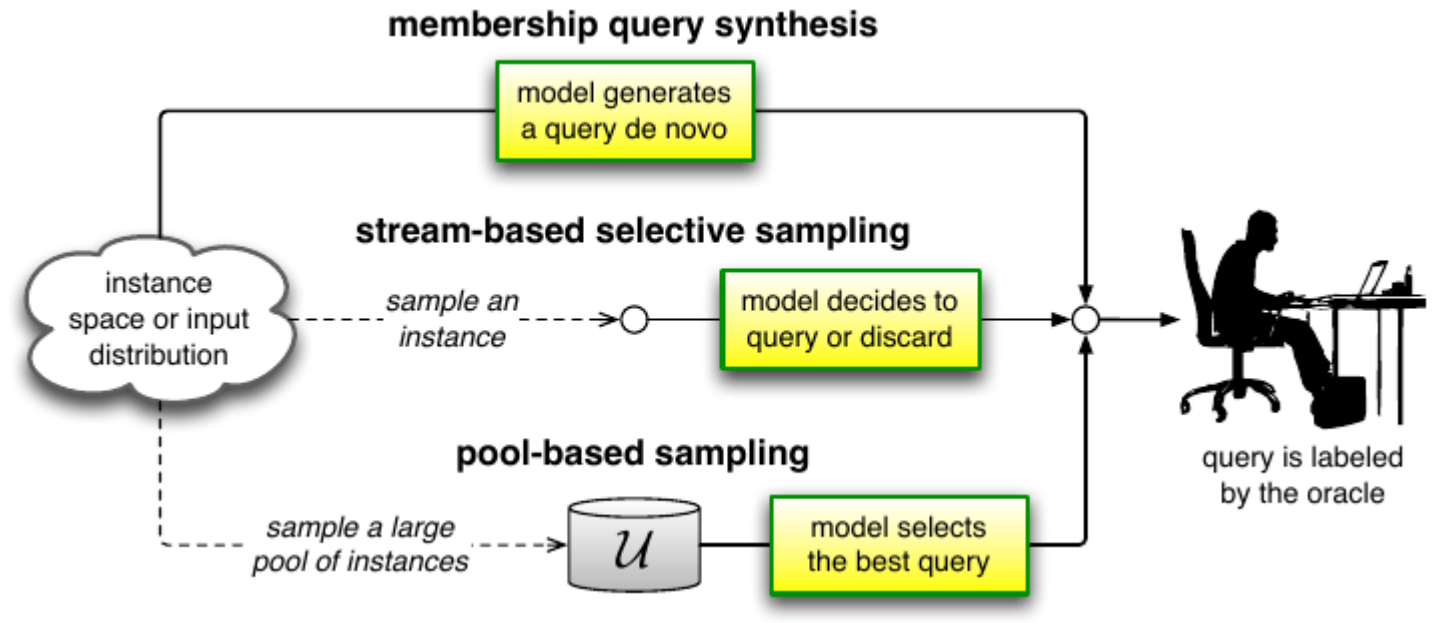
Data Stream Mining



DSM – concept drift

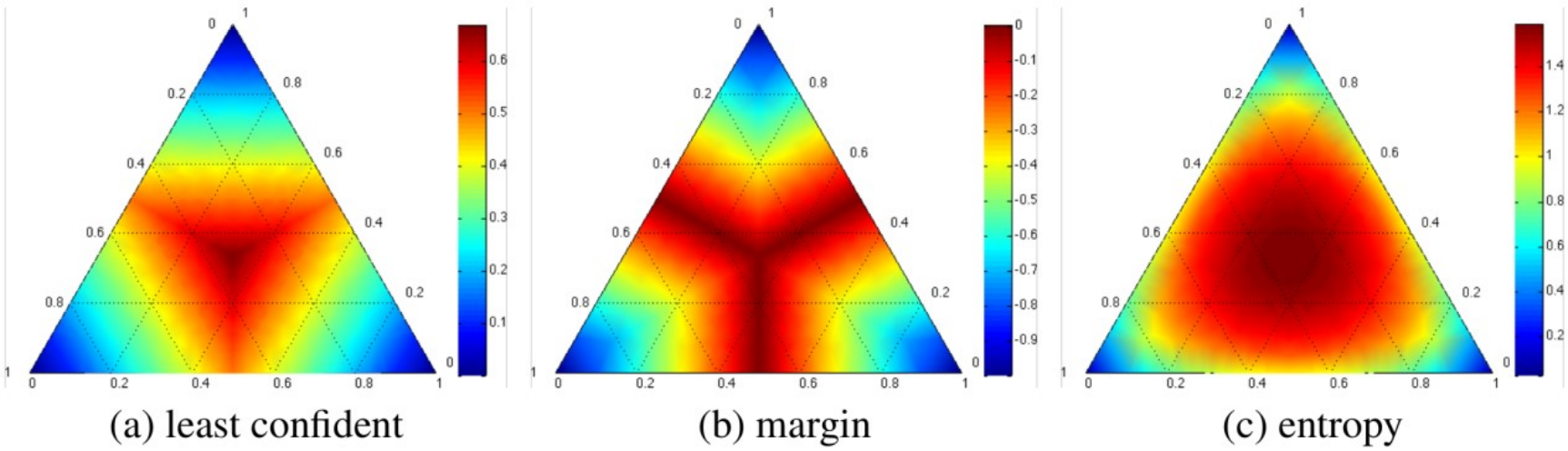


DSM - model (re)training



DSM – Active Learning

Uncertainty sampling



R&D combined

Concepts
- Data stream mining
- Active Learning

Resource
- Data probes / sinks everywhere
- Private HPC clouds on premises

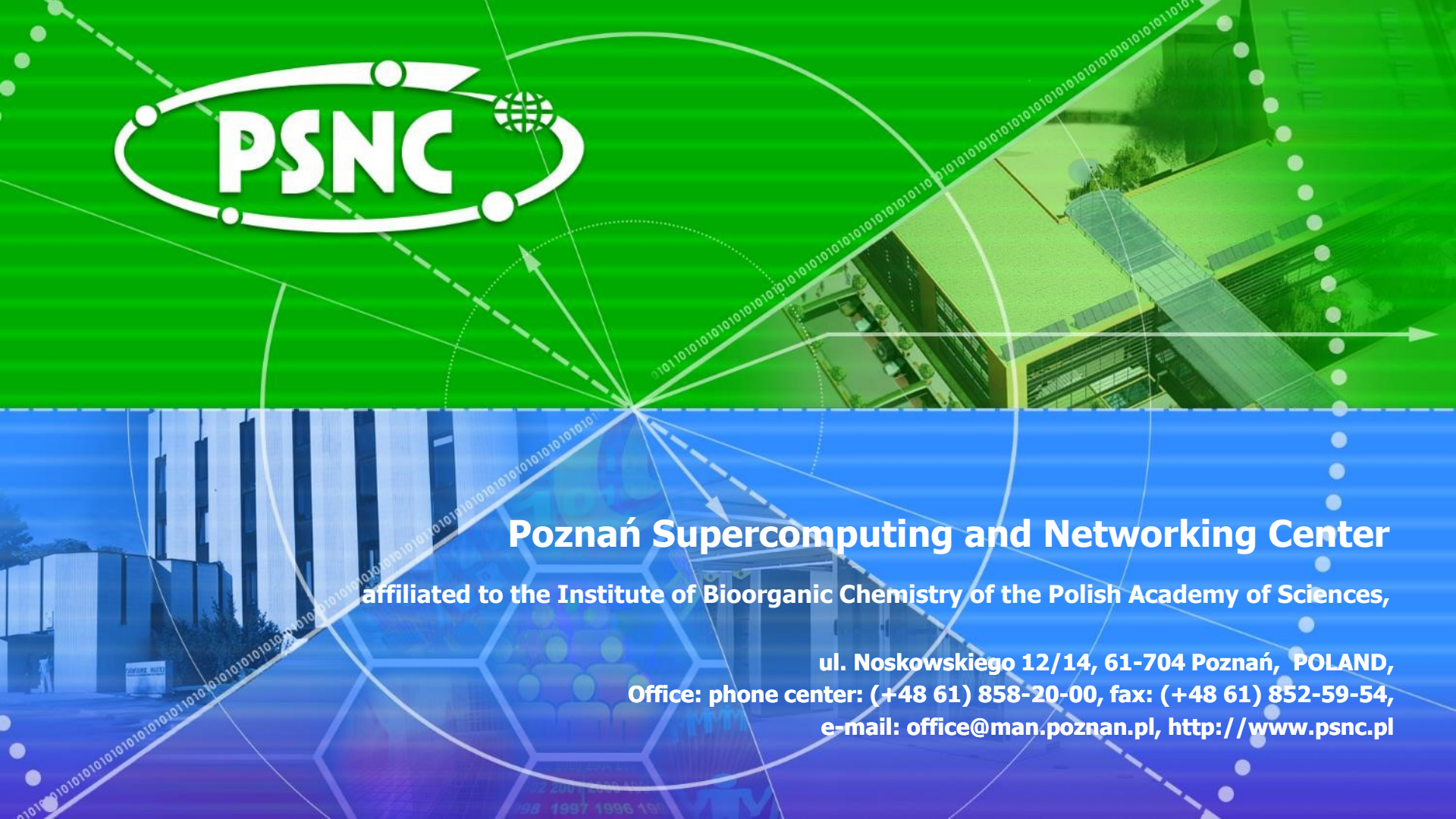
Software
- uServivce / Spring / Netflix OSS / Docker / gRPC
- Apache Spark MLlib / pandas / moa / weka

Summary

- Sophisticated attacks need advanced countermeasures
- It is possible to:
  - Utilize the previous experience in building advanced security solutions
  - Use the HPC infrastructure to significantly increase cybersecurity analytic capabilities
  - Provide advanced SOC-like services for public institutio
    - Outsourcing of advanced security analytics
- We encourage public sector entities to cooperate

Questions?

mikolaj.dobski,
gerard.frankowski,
meyer,
maciej.milostan,
marek.pawlowski,
blazej.pelichowski
[@man.poznan.pl]



Poznań Supercomputing and Networking Center

affiliated to the Institute of Bioorganic Chemistry of the Polish Academy of Sciences,

ul. Noskowskiego 12/14, 61-704 Poznań, POLAND,
Office: phone center: (+48 61) 858-20-00, fax: (+48 61) 852-59-54,
e-mail: office@man.poznan.pl, http://www.psnc.pl