Network security projects from a CERT perspective

Piotr Kijewski
NASK / CERT Polska

ICT Fair for Trust & Security Research, Olomouc, Czech Rep. 14th May 2009

About NASK/CERT Polska

- **NASK (Naukowa i Akademicka Sieć Komputerowa)**
  - R&D unit set up by Polish government
  - Internet Service Provider
  - Operates DNS registry for .pl TLD
  - Operates CERT Polska

- **CERT Polska**
  - Incident handling for .pl constituency
  - Watch & Warning services
  - Close cooperation with other CERTs under FIRST, ISPs, banks & law enforcement in Poland
  - R&D projects mostly focused on monitoring and security situational awareness, activities that can support a CERT

About CERT Polska

- **Participation in various EU projects**
  - **Current:**
    - WOMBAT (FP7)
    - FISHA (Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks Programme European Commission - Directorate-General Justice, Freedom and Security)
  - **Past:**
    - SPOTSPAM (Safer Internet Programme)
    - eCSIRT.net (FP5)
- **Other projects:**
  - **Arakis (integrated into WOMBAT)**
  - **HoneySpider Network (integrated into WOMBAT)**

WOMBAT: Project Motivation

- **EU 7th FRAMEWORK PROGRAMME (2008-2010)**
- **Worldwide Observatory of Malicious Behaviour and Attack Threats**
- **Cyber-crime becomes harder to battle**
  - Malware specifically designed to defeat today's best practices
  - Organization is consolidating malicious activity into a profitable professional endeavour
- **Data collection and sharing is limited**
  - Collection initiatives are heterogeneous
  - Privacy or confidentiality limits sharing
  - Data structure and analysis remains private
- **No investigation framework exists for consistent and systematic malware analysis**

The WOMBAT Consortium

EURECOM
Sophia Antipolis

orange™

TU WIEN
Technische Universität Wien
Vienna University of Technology

symantec™

HISPASEC SISTEMAS

FORTH

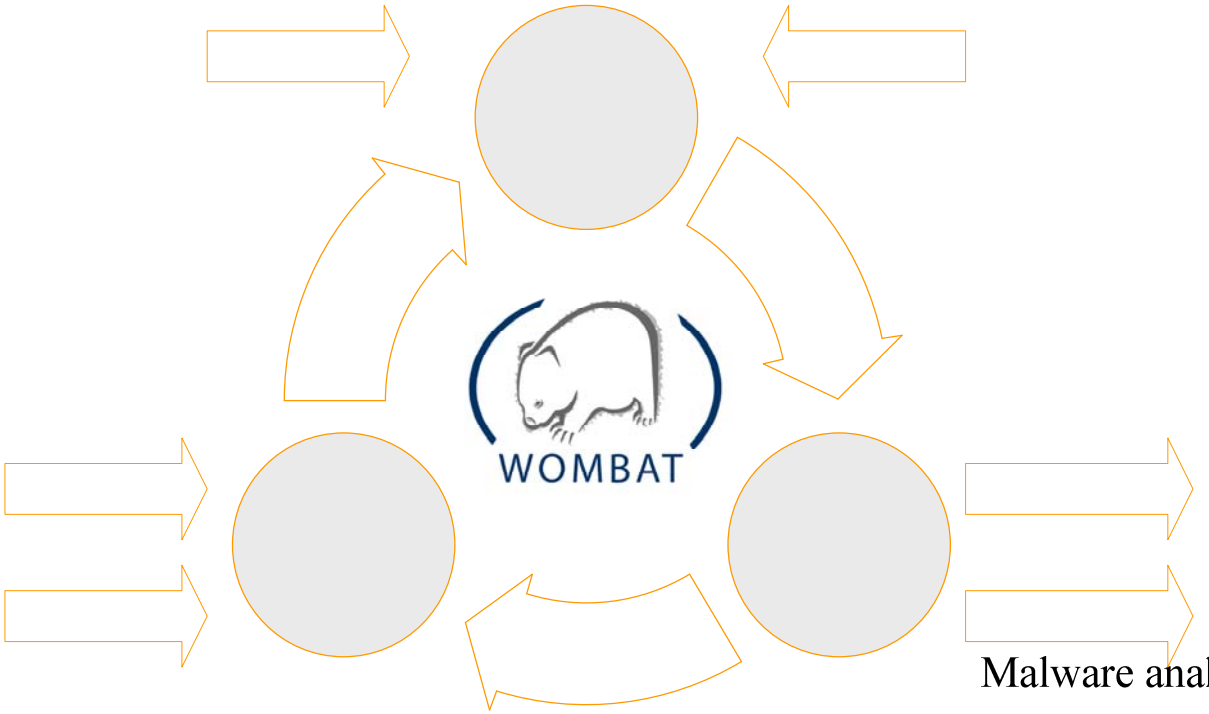
POLITECNICO DI MILANO

vrije Universiteit

NASK

CERT POLSKA

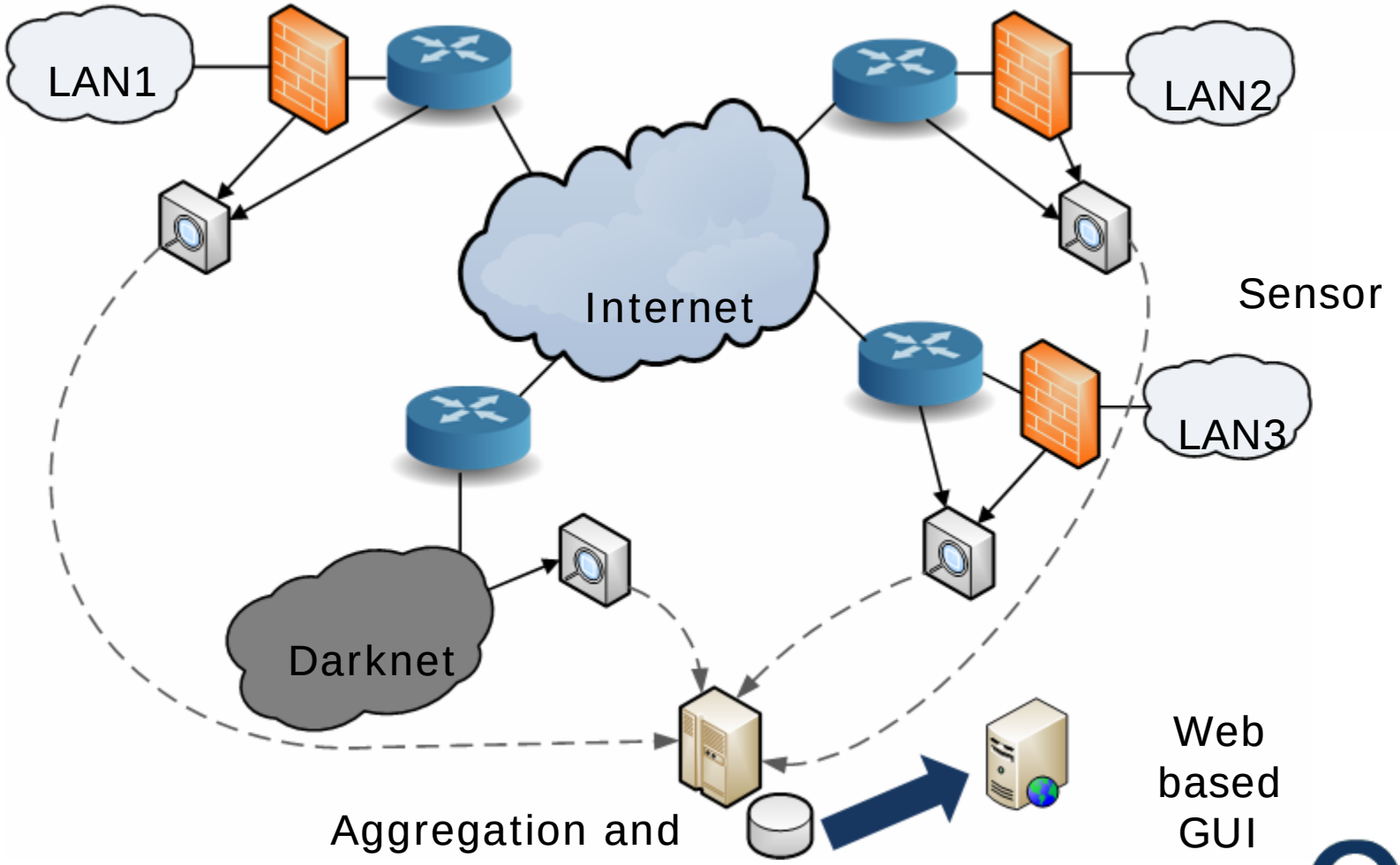
WOMBAT: Main objectives and principles



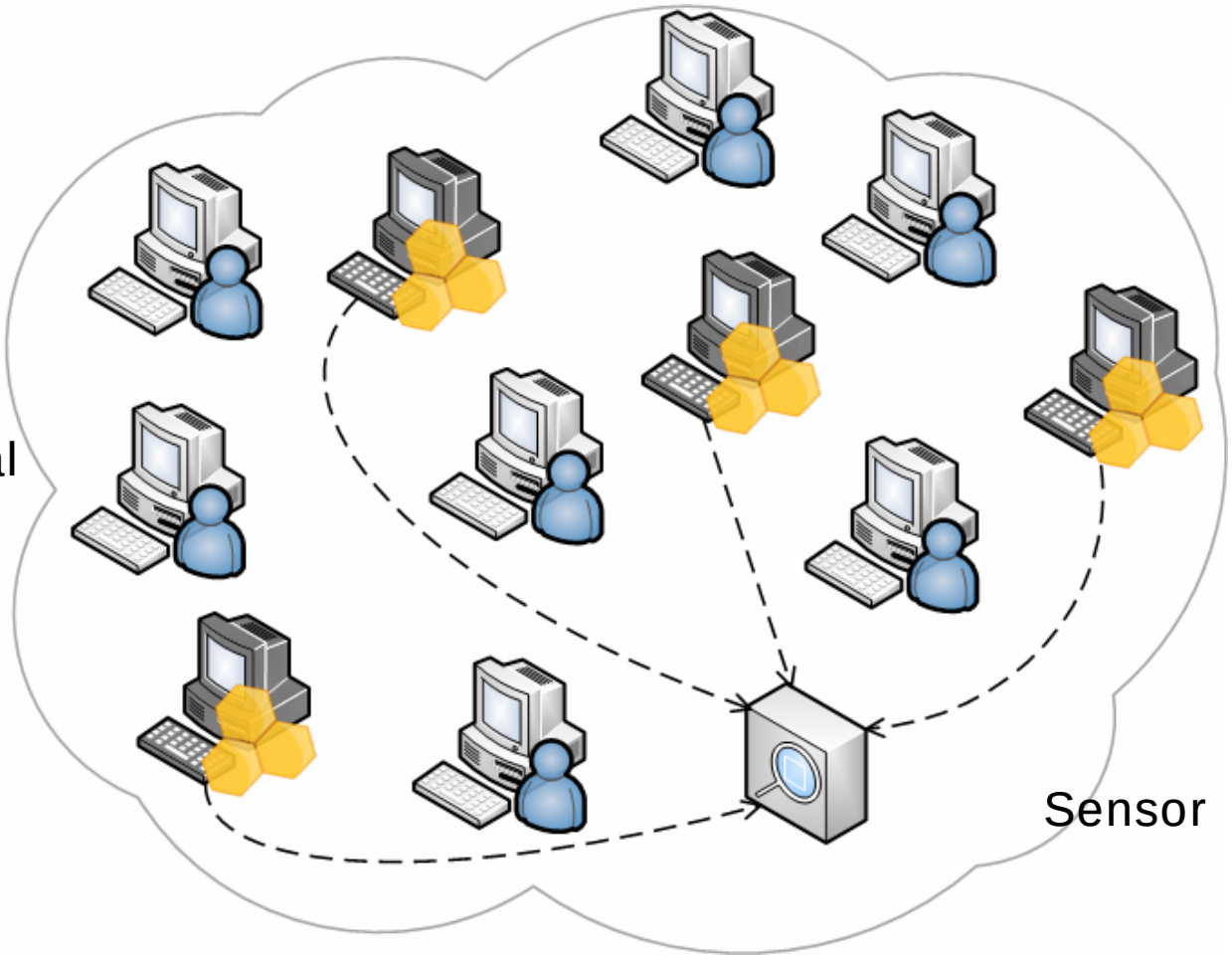
Arakis (1)

- **Early Warning System based on:**
  - honeypots
  - firewalls
  - darknets
  - antivirus reports
- **Automatically detect and characterize threats (including 0days)**
- **Enable trend analysis**
- **Identify targeted attacks**
- **Provide a service to constituents**
- **ARAKIS-GOV implementation jointly with Polish Internal Security Agency – started 2005**
- **Over 50 sensors operational**

Arakis (2)


LAN1
LAN2
Internet
Sensor
LAN3
Darknet
Aggregation and
Analysis Center
Web
based
GUI

Arakis (3)



HoneySpider Network (1)

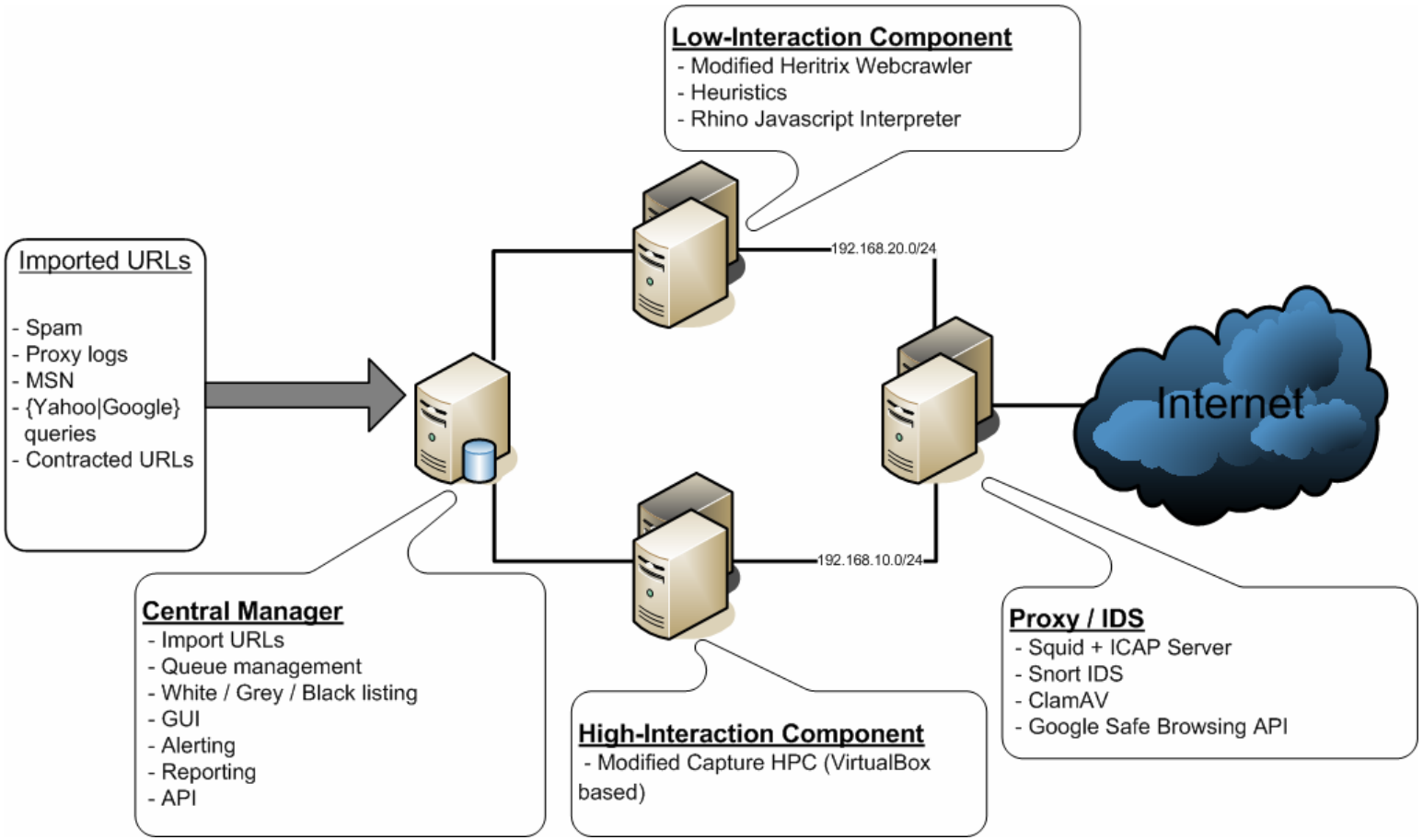
HONEYSPIDER
network

- **Joint effort: NASK/CERT Polska, GOVCERT.NL, SURFnet**
- **Started 2007, working system expected 2009**
- **Goals:**
  - To build a complete, stable and mature client honeypot, capable of processing bulk volume of URLs.
  - To detect and identify URLs which serve malicious content.
  - Detect, identify and describe threats that infect computers through browser technology, such as:
    - Browser (0)-day exploits
    - Malware offered via drive-by-downloads
- **URL: http://www.honeyspider.org**

HoneySpider Network (2)

- **Combination of low-interaction and high interaction client honypots**
- **Low interaction component built around heritrix web crawler:**
  - JavaScript deobfuscation support/Flash support
  - Variety of heuristics, including malicious web pages detection Naive Bayesian algorithm
  - Around 100k urls per day per one low interaction crawler
- **High interaction component based on modified Capture-HPC**
  - Built around VirtualBox
  - Support for running multiple VMs in parallel
  - One instance of the high interaction component around 5-10k urls per day
- **Central manager deals with the URL workflow process: queueing, load balancing etc**

HoneySpider Network (3)



NASK

fisha
A Framework for Information Sharing and Alerting

FISHA (1)

- **Framework for Information Sharing & Alerting**
- **EU Project: DIRECTORATE-GENERAL JUSTICE , FREEDOM AND SECURITY, Specific Programme on „Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks”**
- **Prototype of multi-lingual European Information Sharing and Alert System (EISAS)**
- **Started February 2009**

CERT POLSKA

FISHA (2)

- **Goals:**
  - Improve security awareness amongst home users and SMEs through the creation of a European information sharing and alerting system
  - Create a channel that can be used to reach these groups and supply them with timely best practice information, alerts and warnings phrased in an easy to understand, non-technical way
  - Design and implement the framework:
    - **Set up pilot (N)ISAS systems**
    - **Design and implement protocols for exchange of alerting information**
  - Prepare an awareness campaign
  - Improve cooperation between relevant stakeholders
  - Not compete with existing initiatives (but enable synergy)

FISHA (3) - Partners

Consortium partners

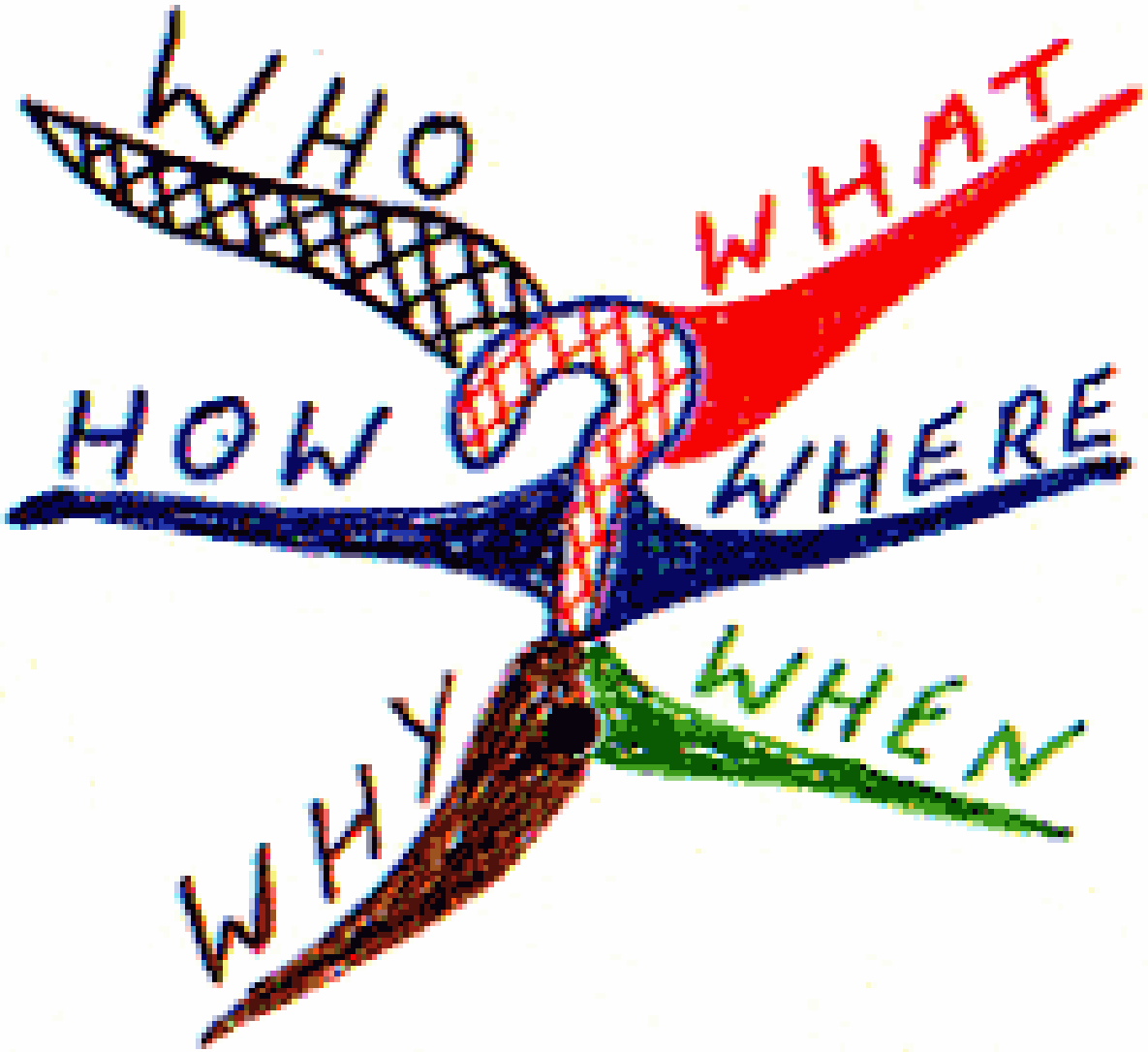
- CERT Hungary
- Research and Academic Computer Network (NASK)
- Internet Security Centre of the University of Gelsenkirchen

Supporting partners

- CERT-FI/Finnish Telecom Agency
- GOVCERT.NL
- The Electronic Government Centre of Hungary
- The Hungarian Telecom Agency
- Cisco Hungary

Future projects:

- **Areas of interest:**
  - Network monitoring & anomaly detection
  - Frameworks enabling automation: malware analysis, data sharing etc
  - Enhancement of threat intelligence methods
  - Identification of malicious activity on the web
  - Honeypot technologies
  - Detection of targetted attacks
  - Digital forensics
  - Cloud computing …


WHO
WHAT
HOW
WHERE
WHY
WHEN