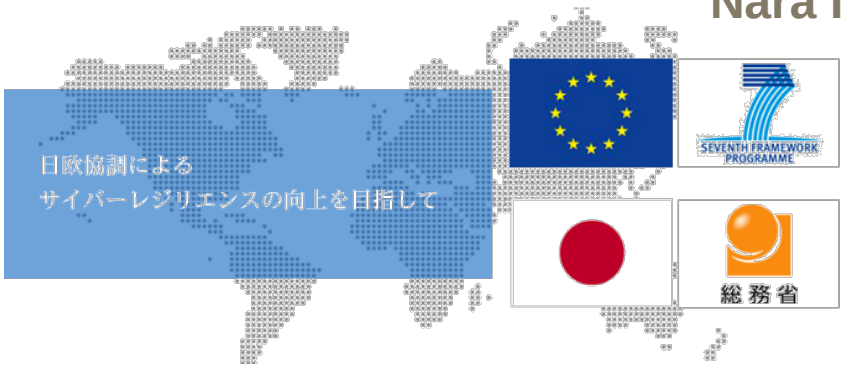
NECOMA

Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis (NECOMA Project)

Director : Youki Kadobayashi
Nara Institute of Science and Technology

Presentator : Yuji Sekiya
The University of Tokyo



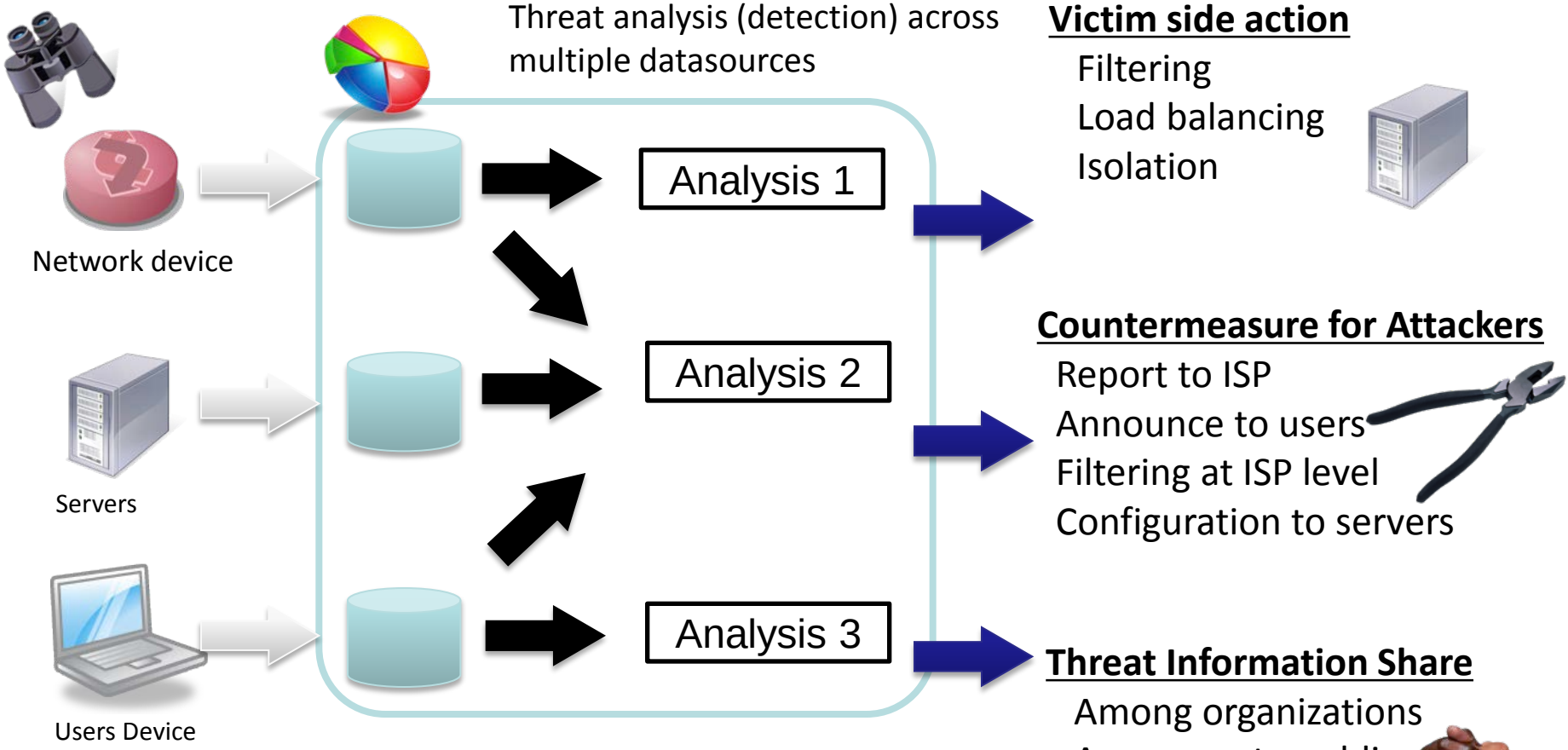
Consortium Members

Hervé Debar (EU lead)	Youki Kadobayashi (Japan lead)
Dawid Machnicki	Kenjiro Cho
Sotiris Ioannidis	Akira Kato
Piotr Kijewski	Romain Fontugne
Jouni Viinikka	Yuji Sekiya

The Goals of NECOMA Project

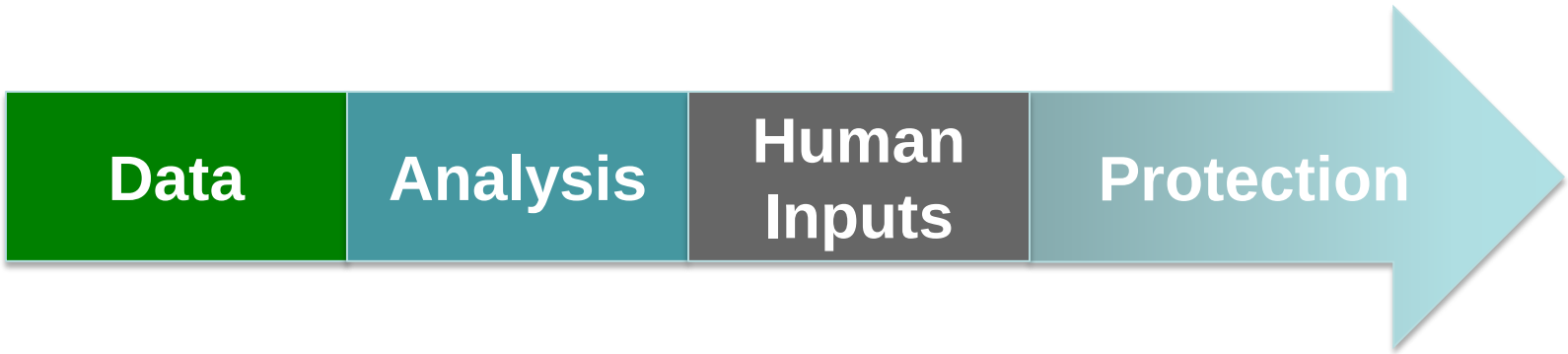
Existing Research	NECOMA	Expected Outcome
Focused to data collection and threat detection.	Focused to threat mitigation and resilience of system.	Actionable Information
Focused to detection of the particular threats.	**Detection threats as mixture of incidents. Multylayer Analysis**	Advanced defense mechanism.
No tight relations among data collection, analysis, and defense.	**Pipeline and Automation.**	Pipeline from data collection to mitigation.

Multi-layer Threat Analysis

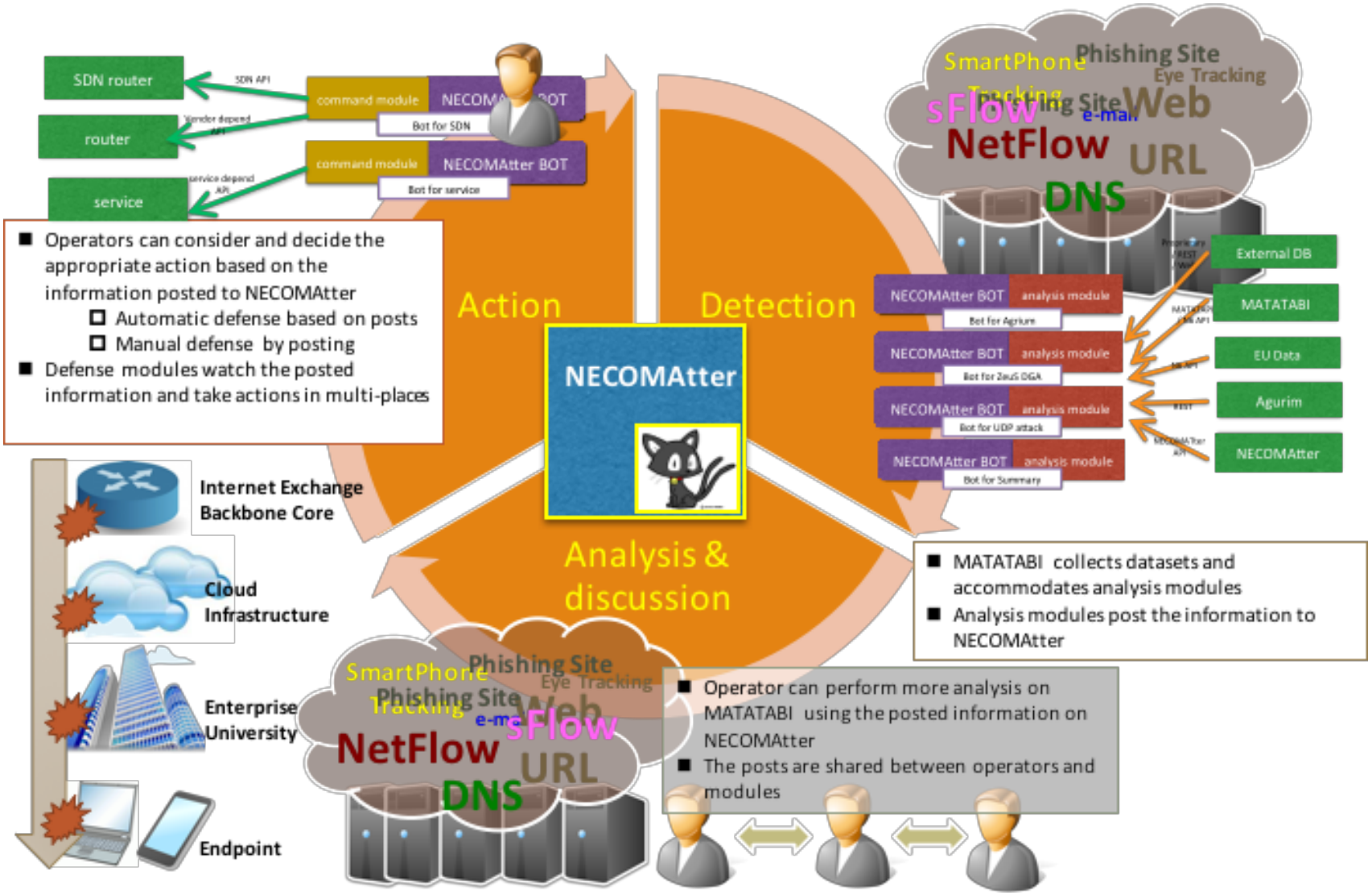


Security Information Pipeline

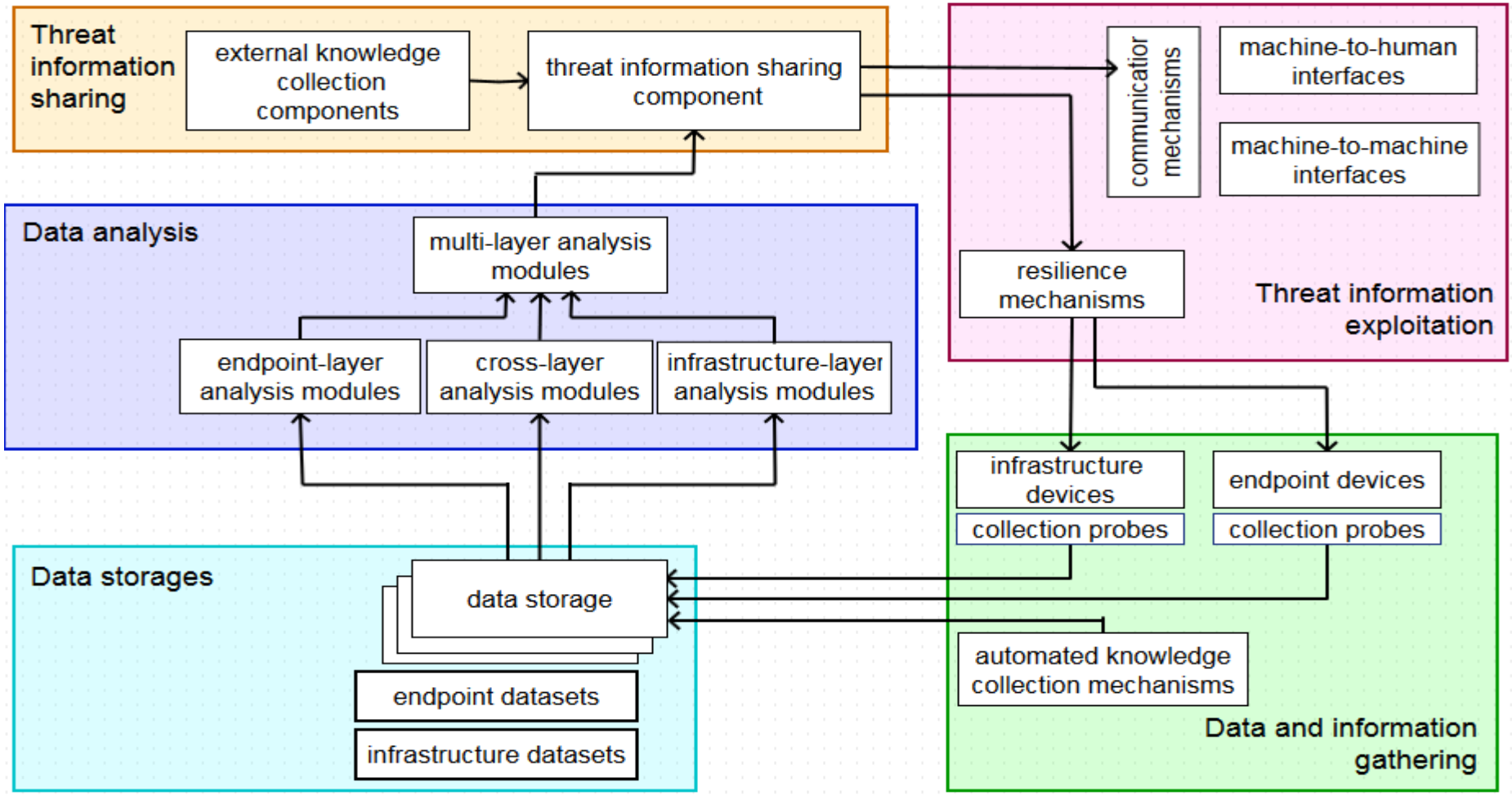
- Making *pipeline* through divert activities
  - Data collection (Traffic, User behavior, etc)
  - Threat Analysis
  - Human decision
  - Protection (Enforcement)



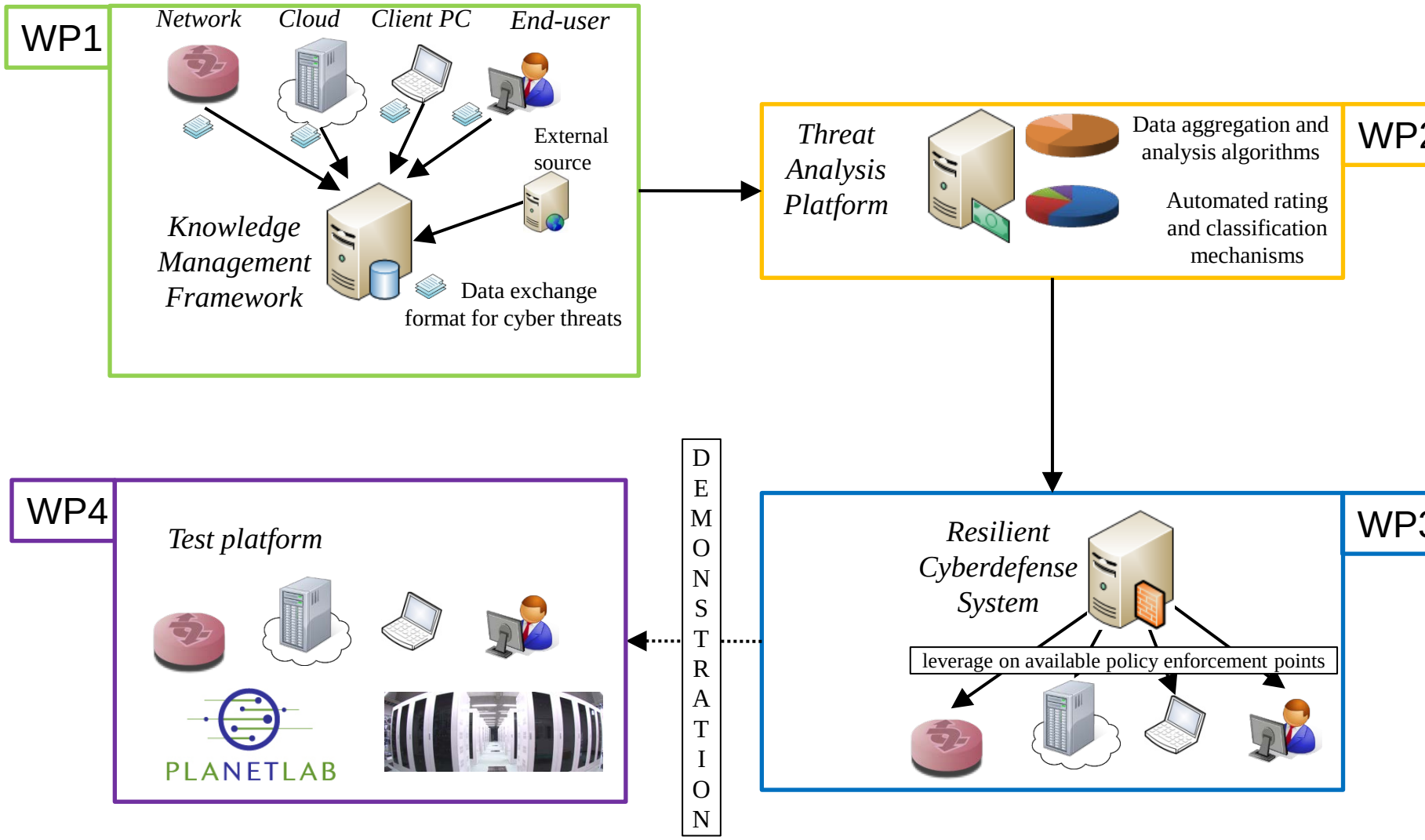
NECOMA Eco-System



NECOMA Architecture



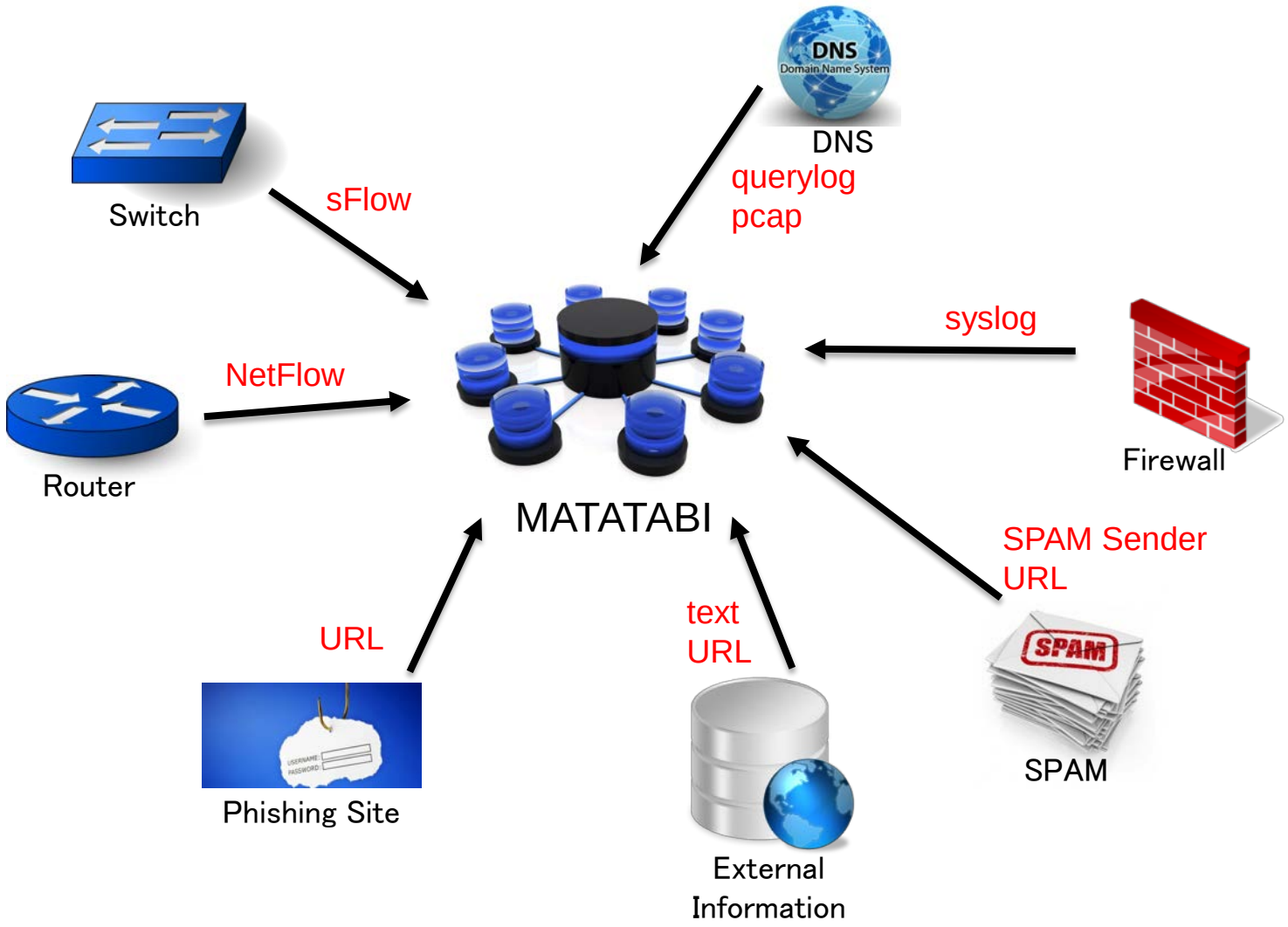
NECOMA Work Packages



Major Achievements

- WP1
  - MATATABI : Data Collection and Threat Analysis System
- WP2
  - NECOMAtter : Threat Information Exchange and Pipeline System
- WP3
  - SDN-IX : Cyber-Threat Defense at the Internet Core
  - Hashdoop : Anomaly Detection Mechanism based on Network Traffic Behavior
  - Cloud Defense : Threat Detection and Defense Mechanism for Public and Private Cloud
  - Endpoint Defense : Mitigation Mechanism in Wireless Access Point
  - Human Behavior : Software Plugins to Protect Users from Phishing
- WP4
  - Demonstration Videos for Use Cases on youtube
  - Liaison meetings with Operators and Companies
  - Summer School for Students
  - RAID2015, BADGERS 2015 : International Conference

WP1 : MATATABI

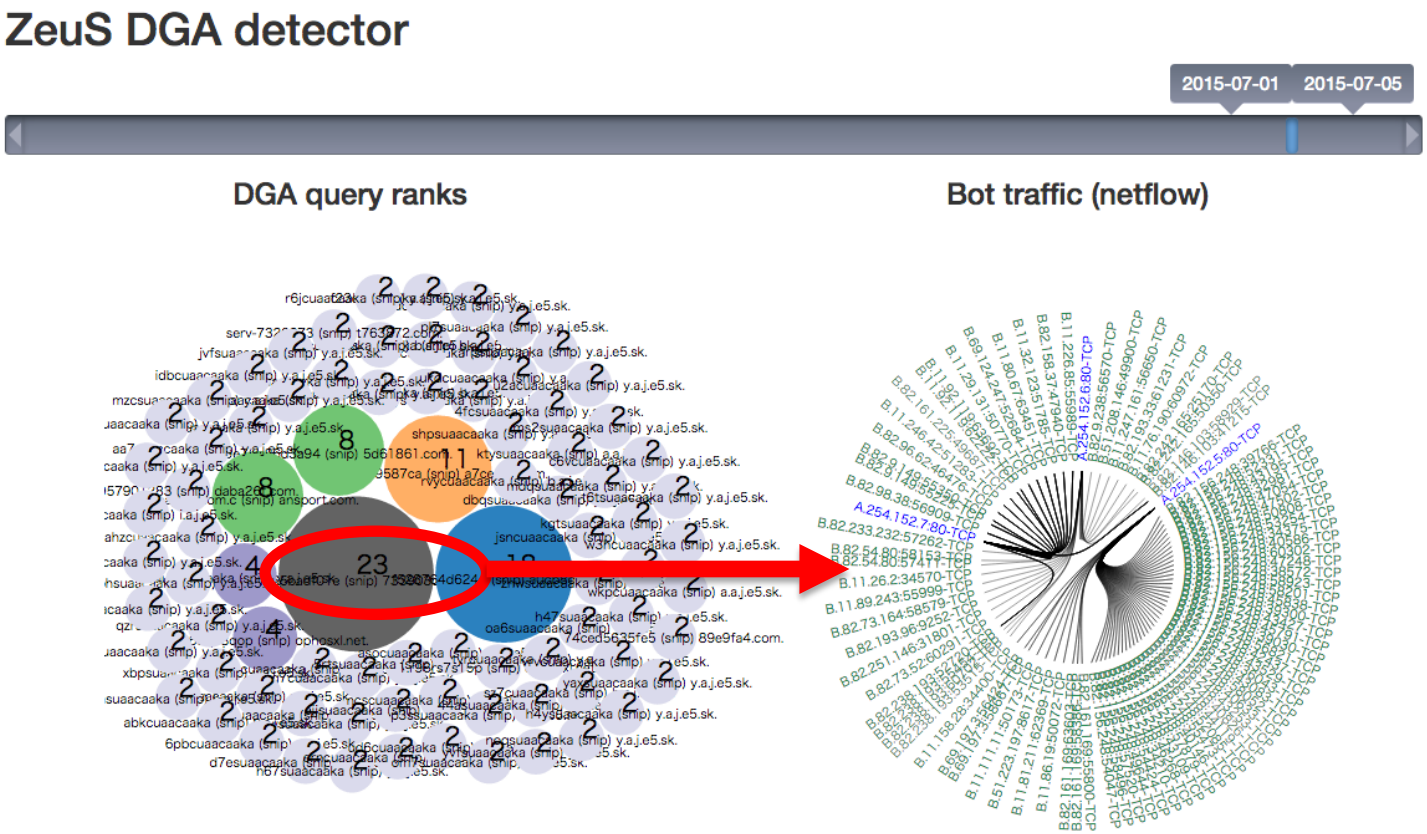


WP2 : Analysis

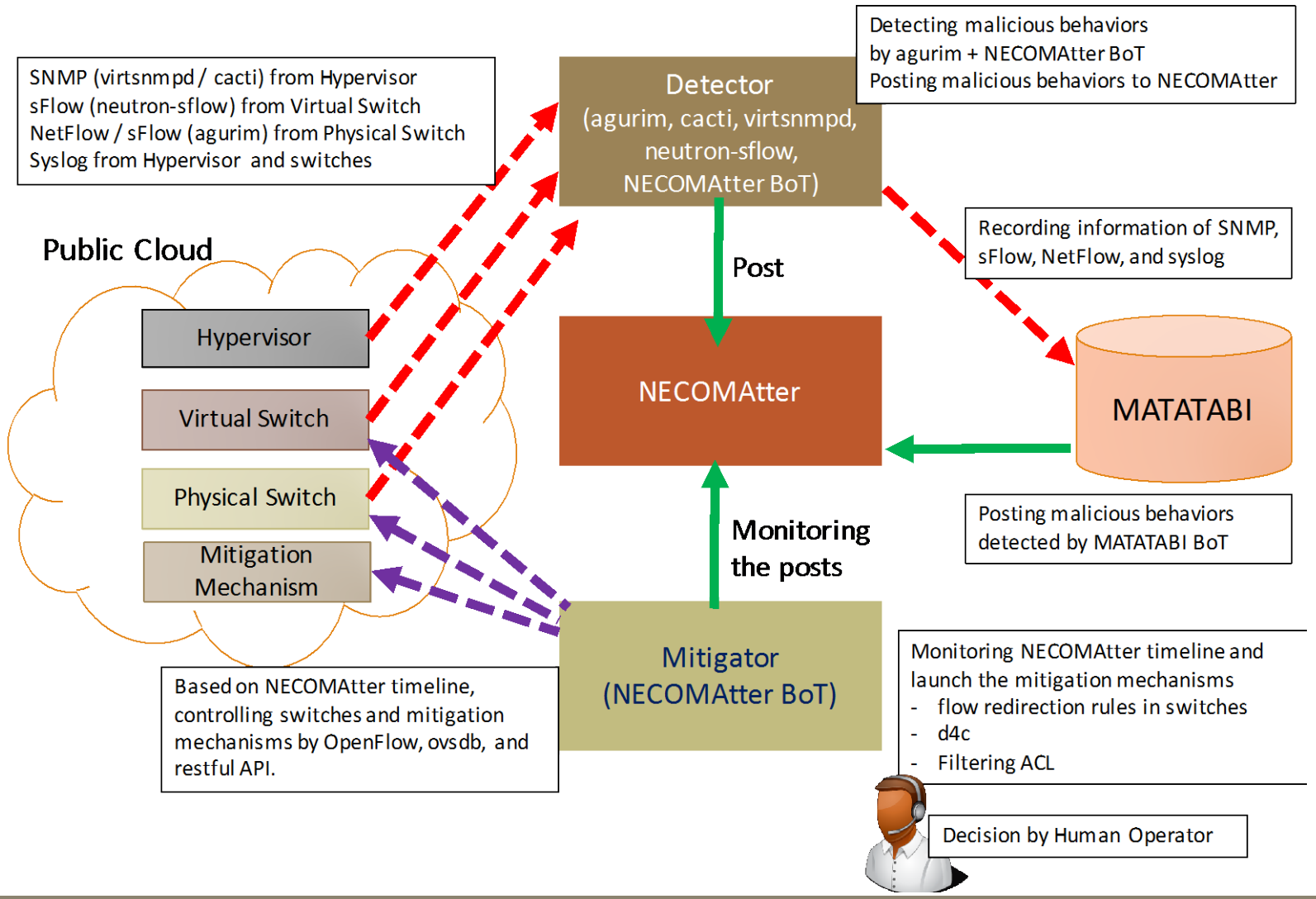
Name	Datasets	Frequency	LoC (#lines)	Remark
ZeuS DGA detector	DNS pcap, netflow	daily	25	hadoop-pcap
UDP fragmentation detector	sflow	daily	48	
Phishing likelihood calculator	Phishing URLs, Phishing content	1-shot	–	Mahout (RandomForest)
NTP amplifier detector	netflow, sflow	daily	143	pyhive, Maxmind GeoIP
	sflow	daily	24	
DNS amplifier detector	sflow, open resolver [19]	daily	37	
Anomalous heavy-hitter detector	netflow, sflow	daily	106	pyhive
DNS anomaly detection	DNS pcap, whois, malicious/legitimate domain list	daily	57	hadoop-pcap, Mahout (RandomForest)
SSL scan detector	sflow	1-shot	36	
DNS failure graph analysis	DNS pcap	daily	159	pyhive

WP2 : Visualization of Zeus DGA and Botnet

- 2015/07/01 – 2015/07/05
  - The number of the most active DGA query is 23
  - Related traffic flows from netflow datasets.

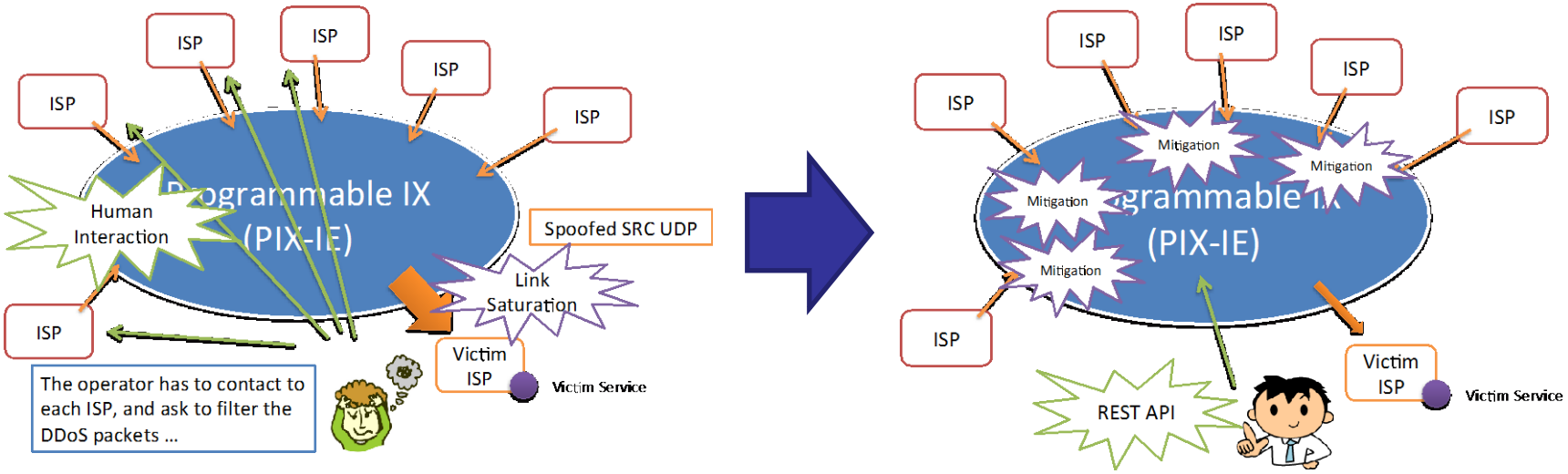


WP3 : Resilient Defense in Public Cloud



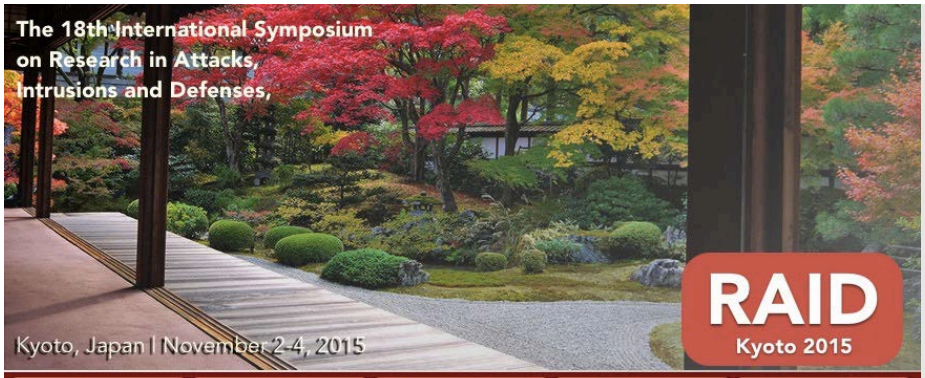
WP3 : Defense Mechanism at the Internet Core

- SDN IX (PIX-IE)
  - Programmable IX in Edo : PIX-IE
  - Mitigating and filtering suspicious flows at IX
- IX is a public space in the Internet
  - Before link saturation, an ISP operator can stop DDoS flows



WP4 : Liason Meeting

WP4 : RAID 2015, BADGERS 2015 in Kyoto



Home | Hotel | Venue and Travel | Registration | Sponsorship
Call for Papers | Program | Speakers | Committees | Contact

Research in Attacks, Intrusions and Defenses (RAID) Symposium

Conference dates November 2-4.

The 18th International Symposium on **Research in Attacks, Intrusions and Defenses**, previously known as Recent Advances in Intrusion Detection, will be held in Kyoto, Japan.

This symposium brings together leading researchers and practitioners from academia, government, and industry to discuss novel security problems, solutions and technologies related to intrusion detection, attacks and defenses.

Committees

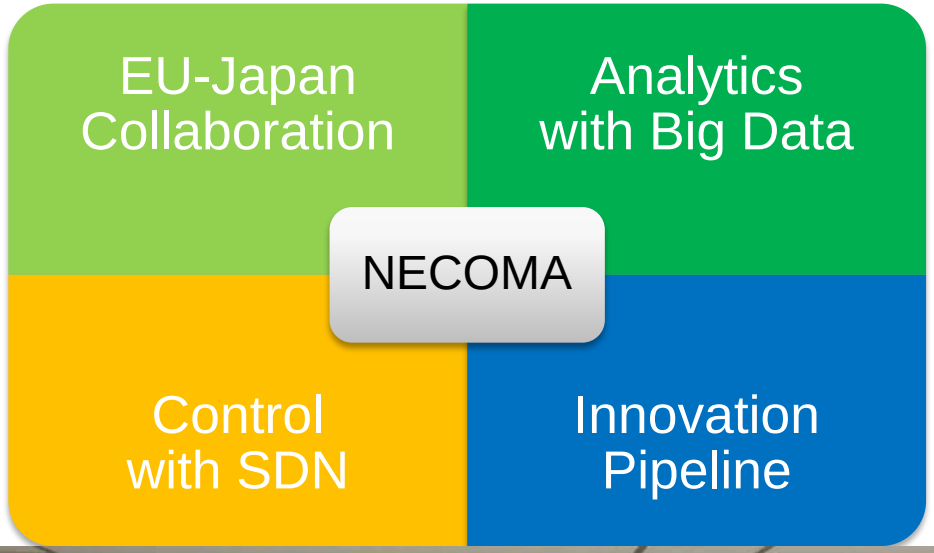
Organizing Committee

General Chair:	Youki Kadobayashi, NAIST
Local Arrangement Chair:	Kazuya Okada, NAIST
PC Chair:	Herbert Bos, Vrije Universiteit/VU University Amsterdam
PC Co-Chair:	Fabian Monrose, University of North Carolina at Chapel Hill
Publication Chair:	Gregory Blanc, Telecom SudParis
Publicity Chair:	Giorgos Vasiliadis, FORTH

Program Committee

- Manos Antonakakis Georgia Tech
- Elias Athanasopoulos FORTH
- Herbert Bos Vrije Universiteit / VU University Amsterdam
- Gabriela Ciocarlie SRI International
- Lucas Davi Intel CRI-SC at TU Darmstadt
- Tudor Dumitras University of Maryland
- Petros Efstathopoulos Symantec Research Labs
- William Enck North Carolina State University
- Bryan Ford EPFL
- Aurélien Francillon Eurecom
- Flavio Garcia University of Birmingham
- Chris Kanich University of Illinois at Chicago
- Christopher Kruegel UC Santa Barbara
- Andrea Lanzi U. of Milan
- Corrado Leita LastLine, Inc.
- Brian Levine UMass Amherst
- Fabian Monrose University of North Carolina at Chapel Hill.
- Zachary Peterson Cal Poly, San Luis Obispo
- Georgios Portokalidis Stevens Institute of Technology
- Niels Provos Google
- Konrad Rieck University of Göttingen
- William Robertson Northeastern University
- Christian Rossow Saarland University
- Andrei Sabelfeld Chalmers
- Stelios Sidiroglou-Douskos MIT
- Patrick Traynor U. of Florida
- XiaoFeng Wang Indiana University
- Dongyan Xu Purdue University

Summary



With tremendous success, NECOMA seeks new horizon