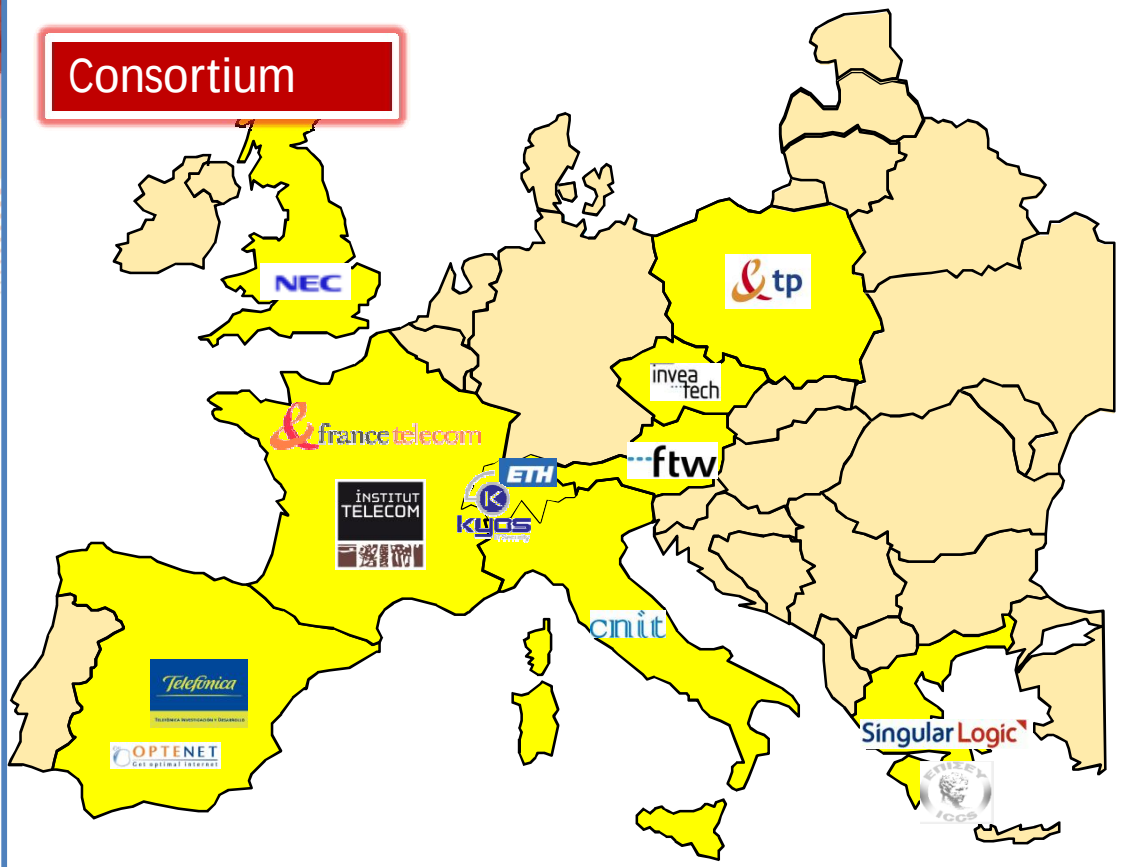
DEMONS
Decentralized, cooperative and privacy preserving Monitoting for trustworthiness

Dr. Sathya Rao
KYOS, Geneva, Switzerland
Sathya.rao@kyos.ch

Introduction

- DEMONS is an integrated project of European FP7 framework partly funded by the European Commission
- Started on Sept. 2010 and will be active for 30 months to achieve its goals
- Has 13 European partners: 3 operators, 6 commercial companies and 4 research institutes
- The budget is 8.3 M€ with EC funding of 5.35 M €
- DEMONS plans to demonstrate the trustworthiness of the inter-domain network monitoring and management infrastructure in a cooperative operational environment

Consortium

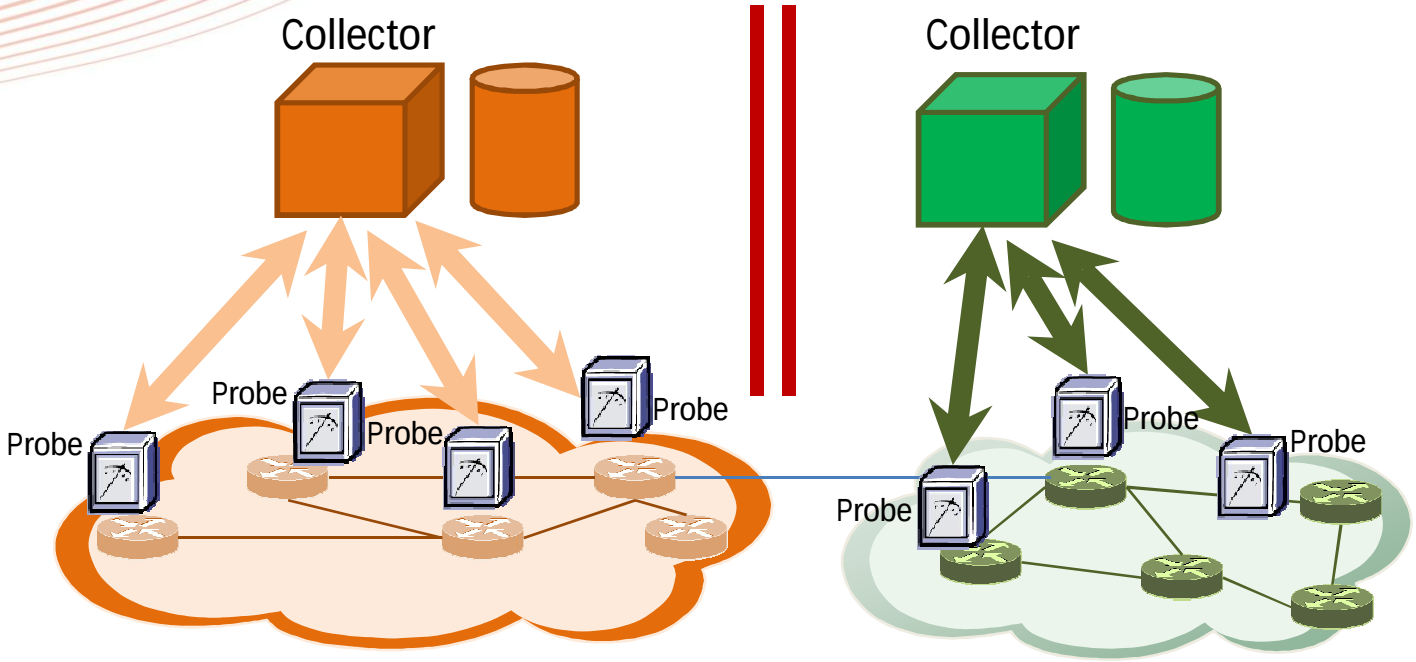


Telefónica I+D, ES
NEC Laboratories Europe, UK
CNIT, IT
FTW. AT
Telekomunikacja Polska, PL
France Telecom, FR
Institut Telecom, FR
ETH Zürich, CH
INVEA Tech, CZ
Singular Logic. GR
ICCS, GR
Optenet, ES
Kyos, CH

SEVENTH FRAMEWORK PROGRAMME

DEMONS

Motivation

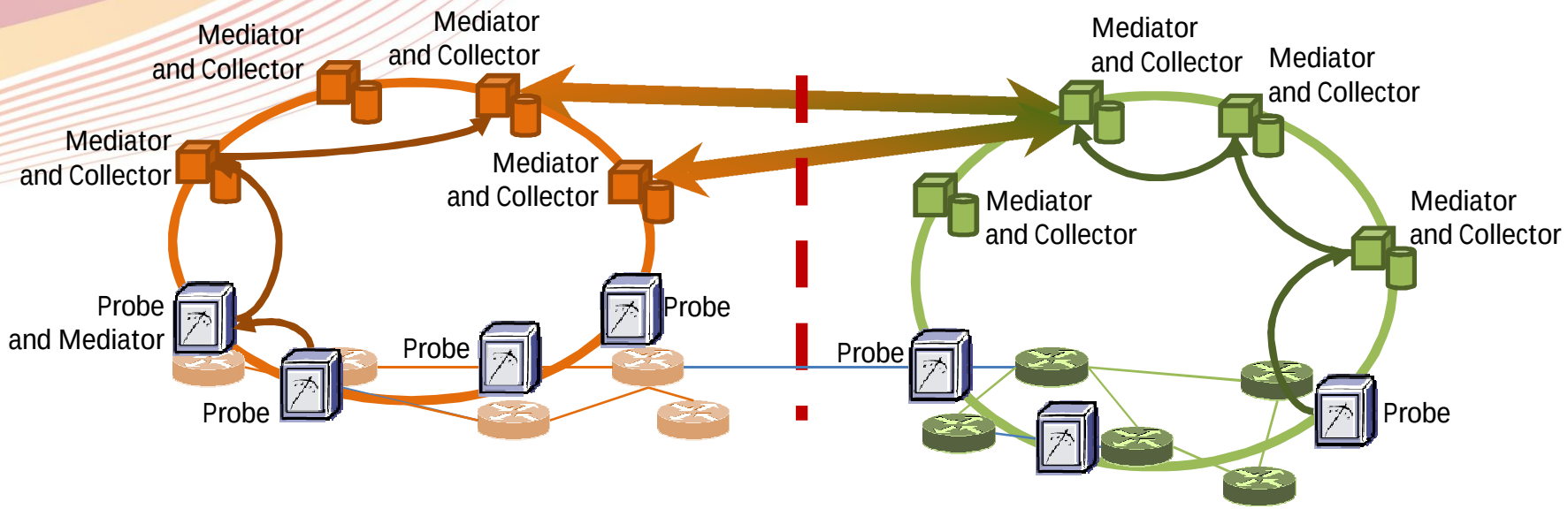


Today's monitoring systems

- Centralized
- Huge amount of exported/collected data
- Hard/no cooperation across domains
- Poor flexibility in access control to monitored data (little more than Y/N)

Hardly coping with
- Higher link rates and traffic volumes
- Networks pervasiveness & capillarity
- distributed, cross-domain, threats

Vision



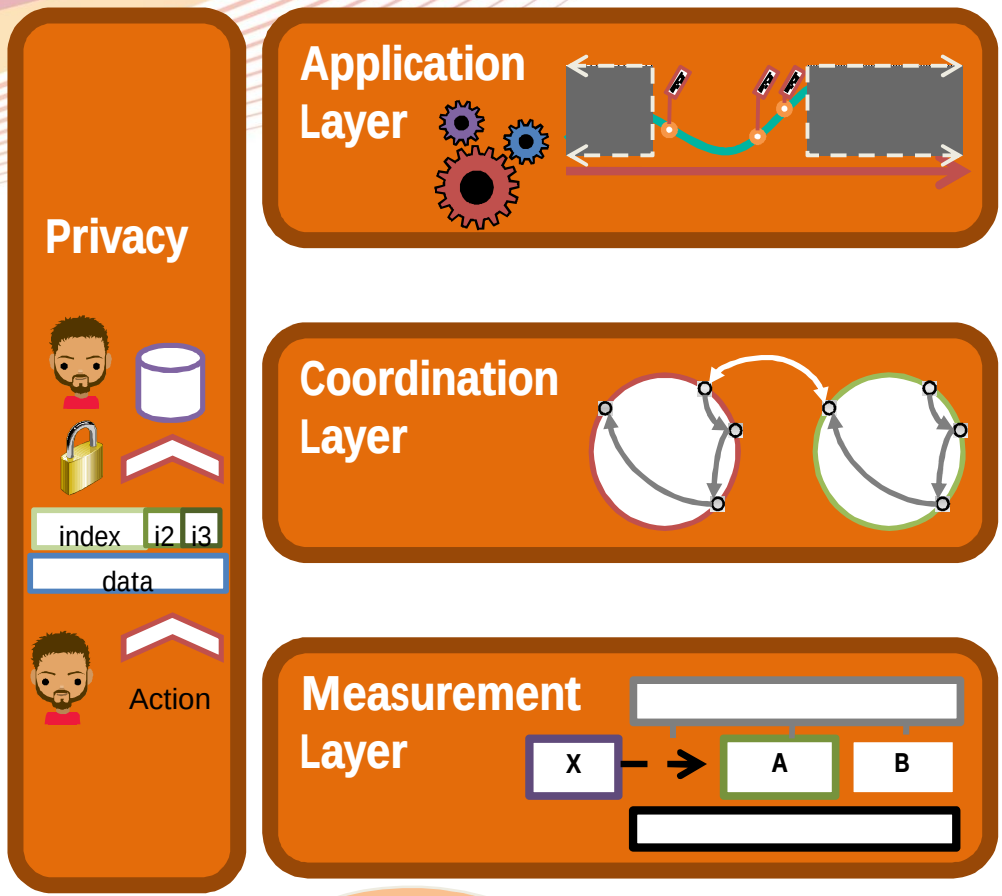
Overlay of in-network monitoring devices

From data-gathering probes to **collaborative P2P computing and filtering devices**

Innovation pillars	Target Impact
In-network processing and distributed intelligence	Scalability
Application-tailored data reduction and protection	Privacy preservation
Resilient autonomic monitoring overlay	Flexibility and resilience
Cross-domain interworking	Cross-domain threat detection and mitigation

Exchange only the information strictly necessary for a given monitoring and analysis objective

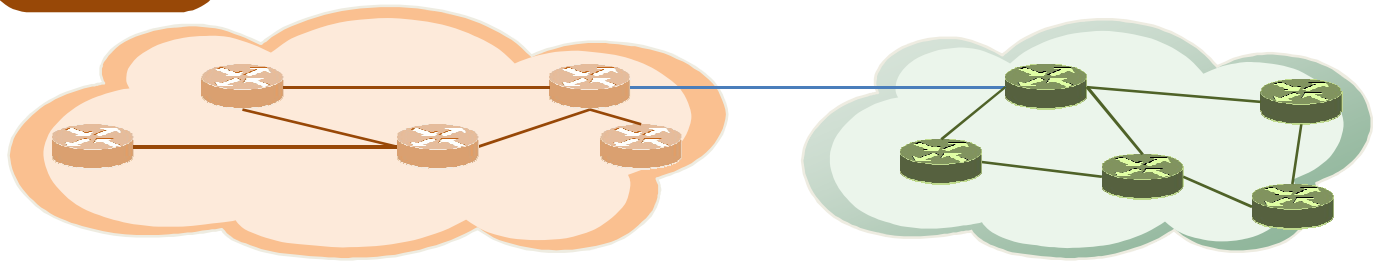
S&T Approach



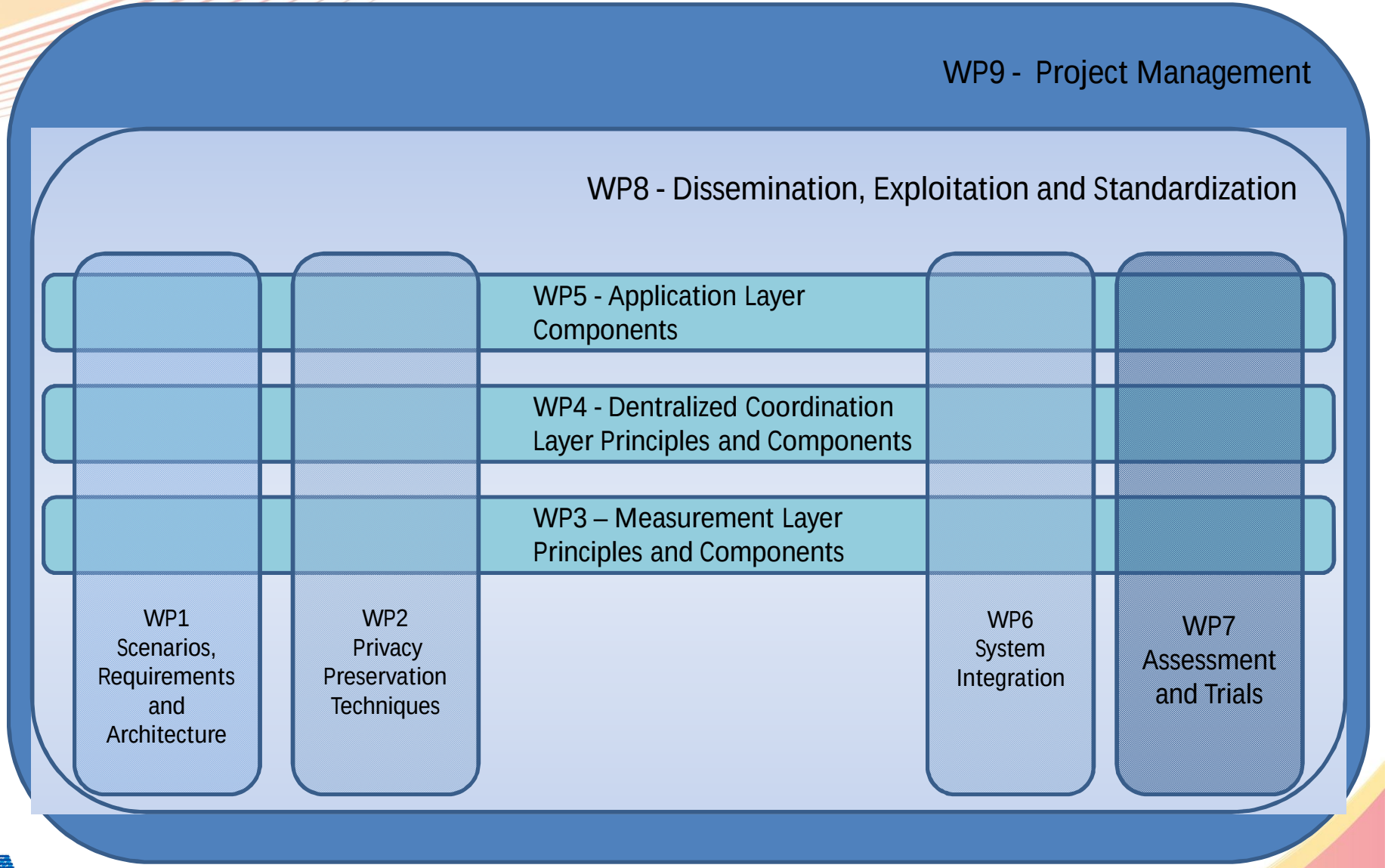
- Cooperative applications
- Application adaptation and deployment
- Presentation & visualization

- Resilient, scalable monitoring overlay
- Orchestration, authorization and control of distributed operation
- Inter-domain cooperation

- In-probe processing and filtering
- Composable traffic analysis tasks
- Flexible & programmable devices



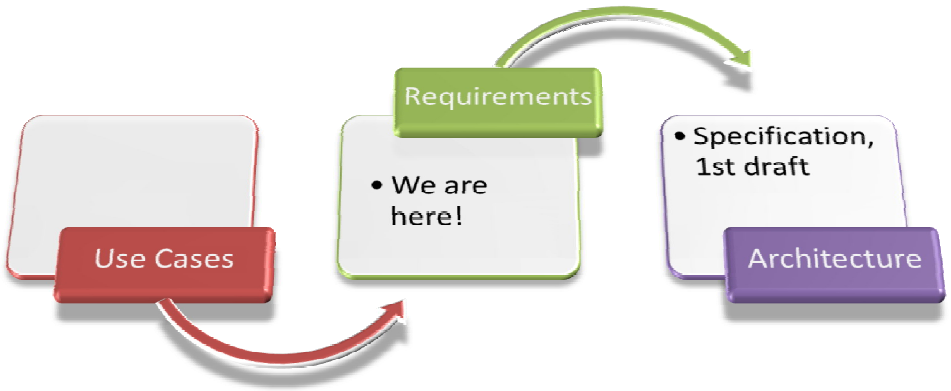
WP structure



Use Cases and Requirements

Activities so far:

- Collect, discuss and write representative use cases depicting current existing problems in the Security (Monitoring) world which DEMONS aims at.
- Extract an initial set of basic requirements for the DEMONS architecture able to address all those scenarios (and more!)

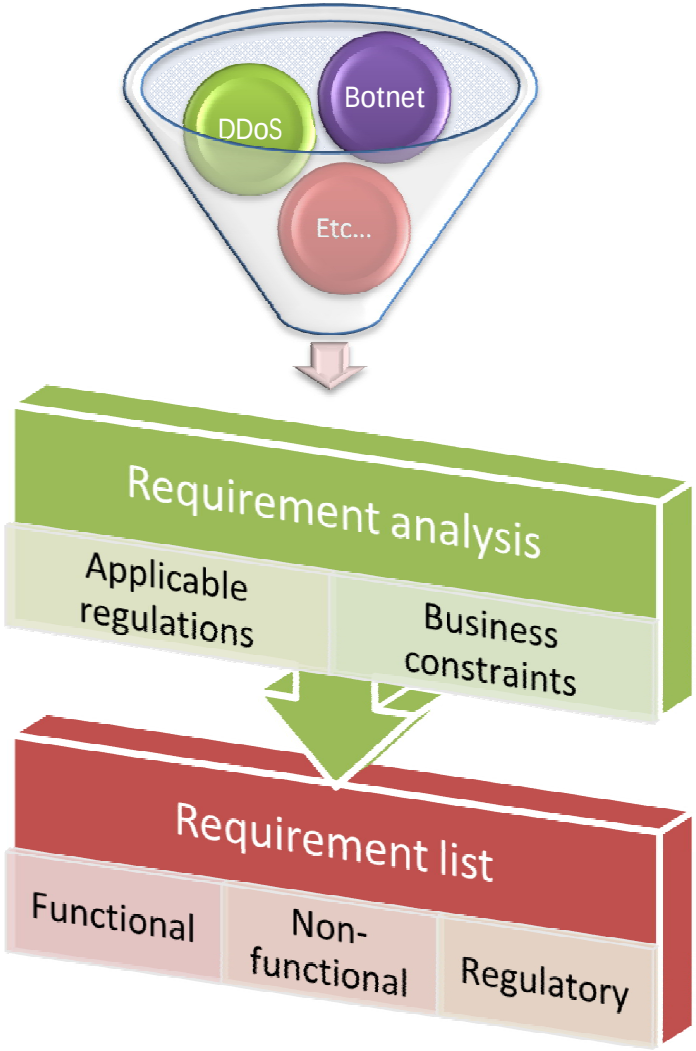


Summary of proposed use cases

- Botnet detection
  - Fast-flux detection
  - Collaboration graph
- Statistical Anomaly detection
- Collaborative IDS
  - Alarm scoring
  - Decentralized filters
- VoIP trustworhiness
- DDoS detection
- Smart grid

Proposed use cases do not cover ALL known security issues but consitutes a balanced set of cases providing a valuable input to build a more general Security Monitoring system

Followed Approach



Summary of Requirements

Functional

- Organizational
- Data input
- Processing
- Information exchange
- Storage

Non Functional

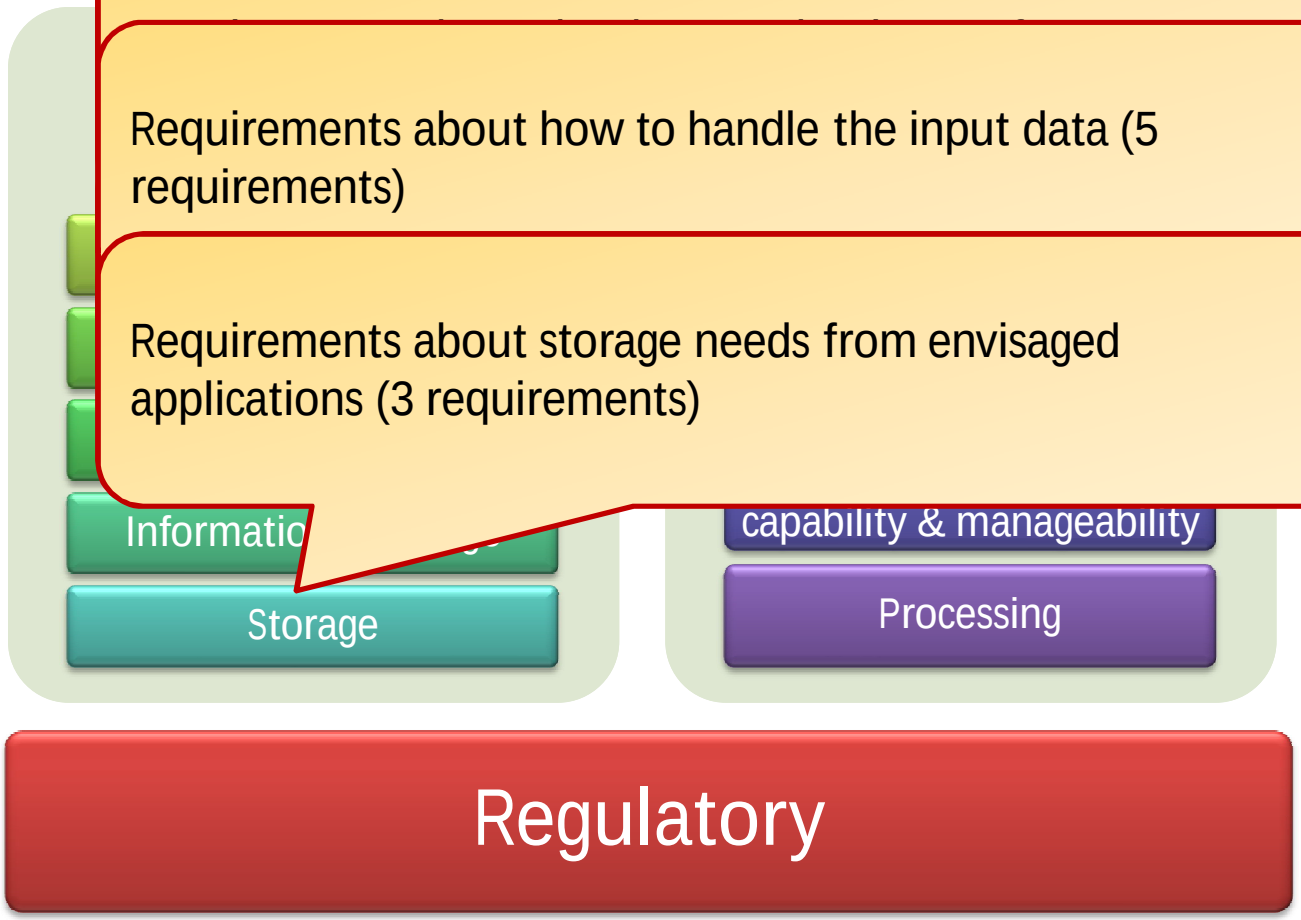
- Organizational
- Performance
- Usability, deployment capability & manageability
- Processing

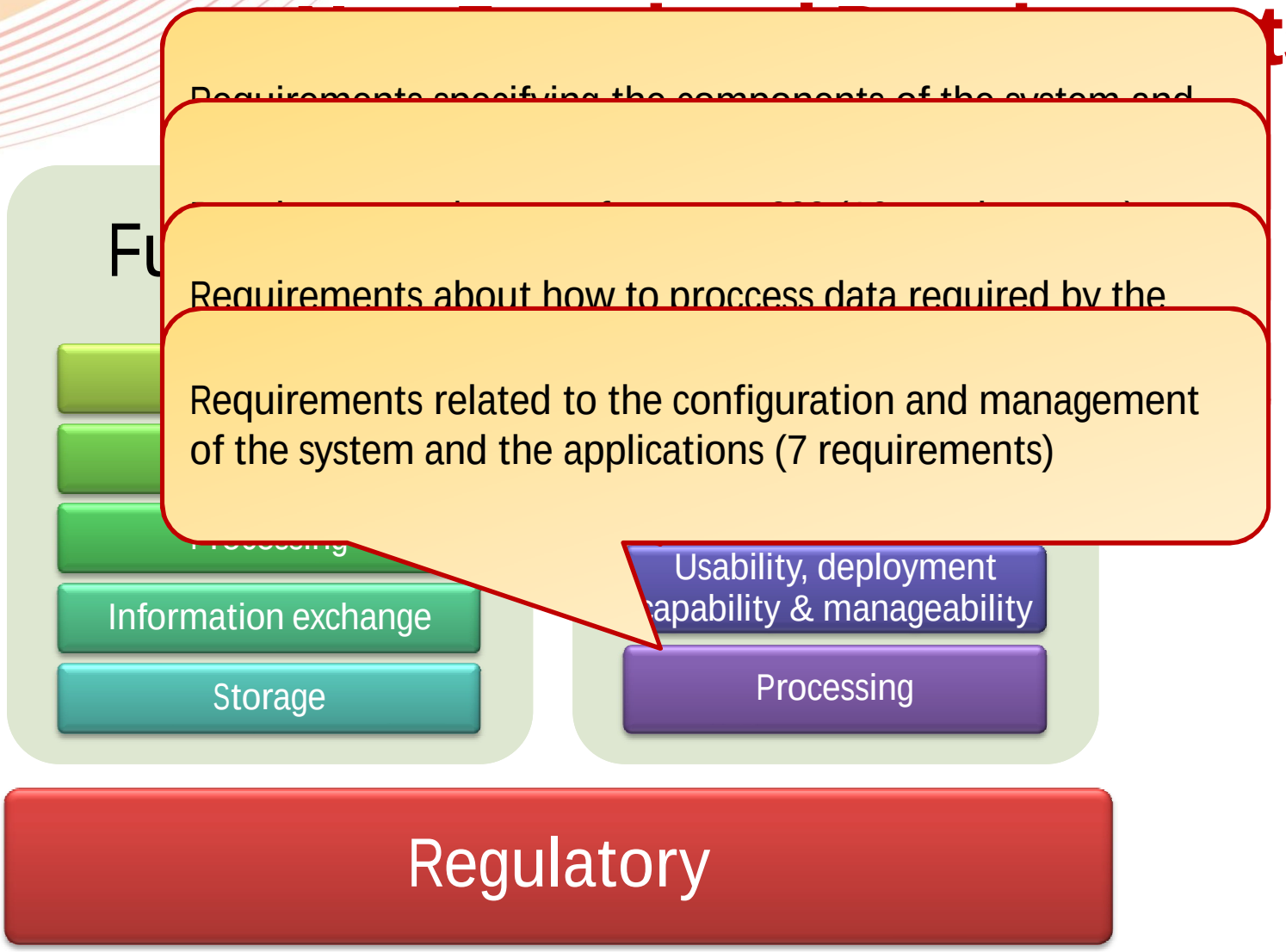
Regulatory

Functional Requirements

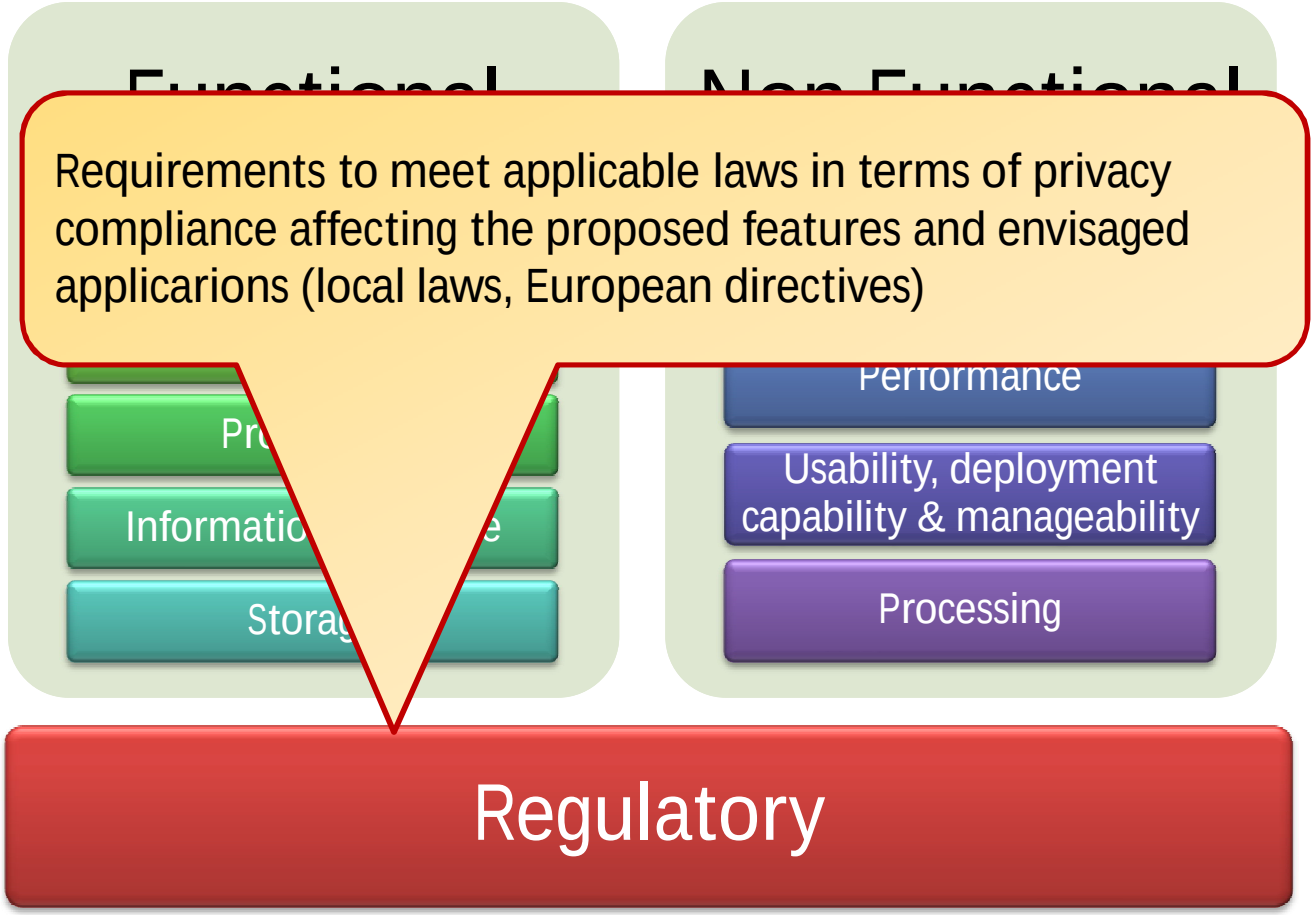
Requirements about how to handle the input data (5 requirements)

Requirements about storage needs from envisaged applications (3 requirements)




Requirements related to the configuration and management of the system and the applications (7 requirements)
Information exchange
Storage
Usability, deployment
apability & manageability
Processing
Regulatory

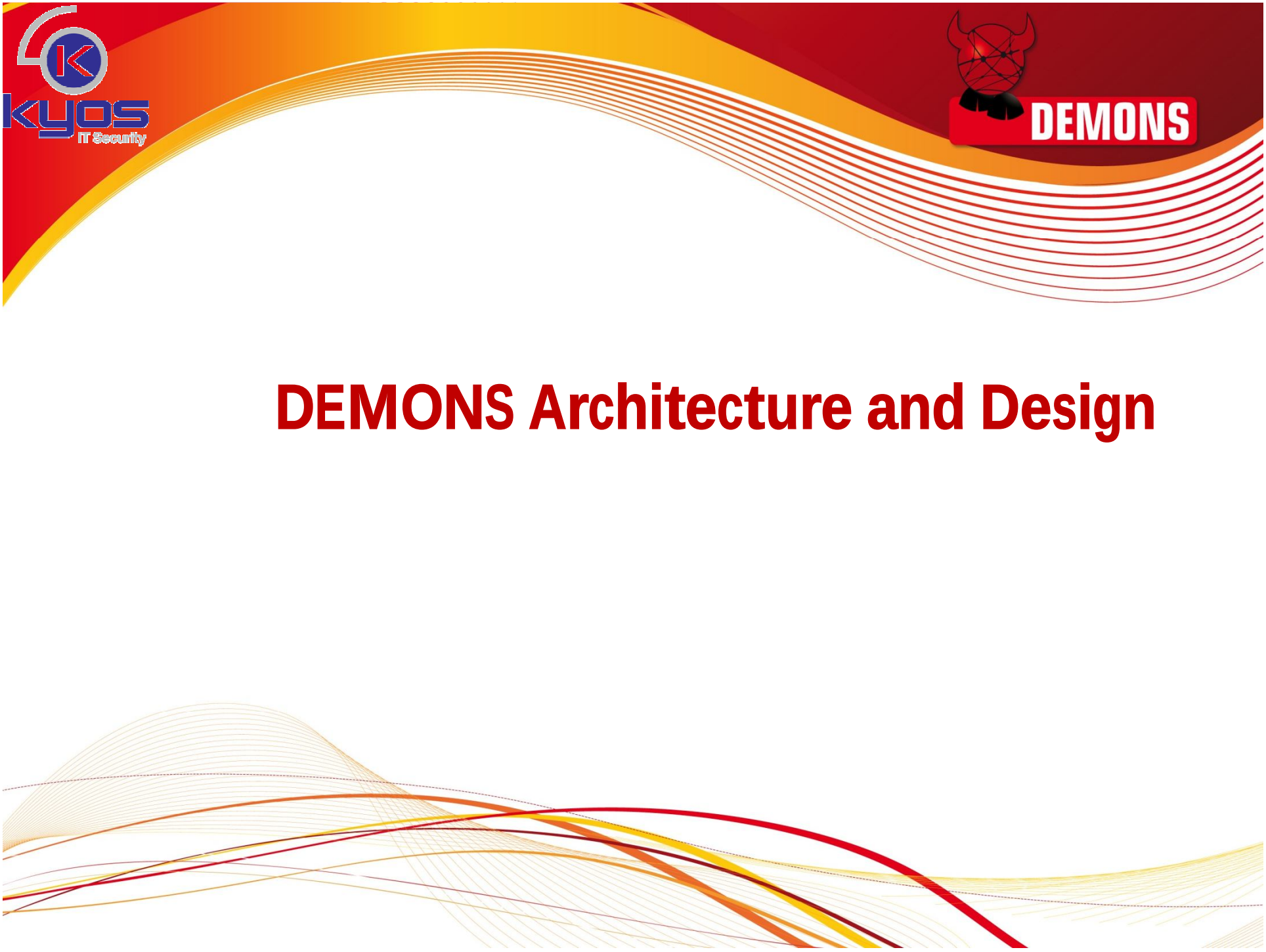
Regulatory Requirements



DEMONS Activities

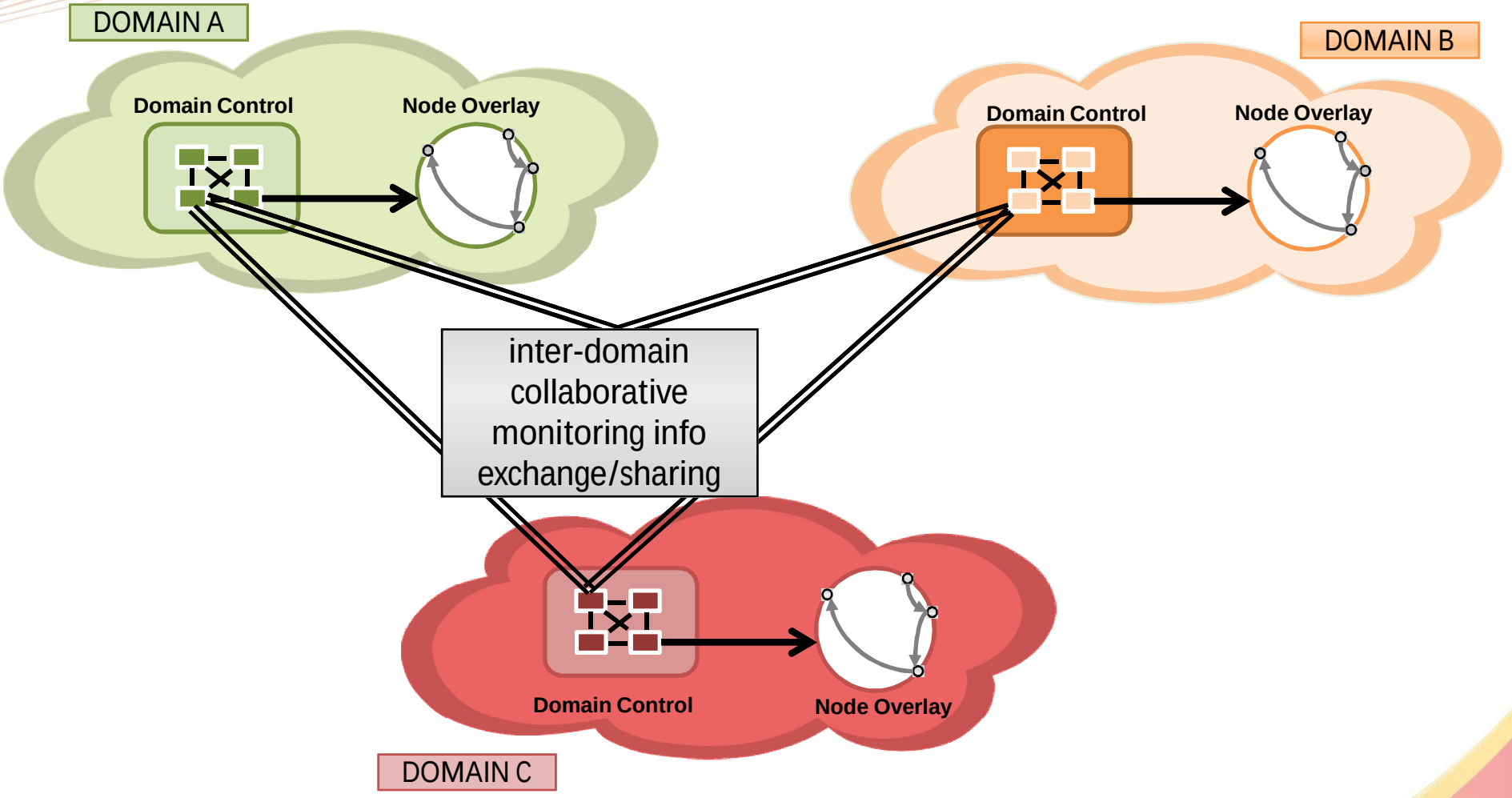
Topics being developed:

- Architecture and initial design
- Authorization and access control models
- In-network traffic processing technologies
- Privacy-enhanced cooperation solutions
- Threat detection and defense solutions (voip, inter-domain, botnet, mitigation)



DEMONS Architecture and Design

DEMONS inter-domain architecture



DEMONS Architecture Principles

- Multiple **simultaneous** applications…
- …defined in terms of composable building **blocks.**
- Infrastructure which adapts to network load and available data.
- Cooperation among domains for data anayalsis and mitigation.
- Application of privacy-enhancing technologies and principles of privacy preservation
- Integration with existing operator infrastructure.

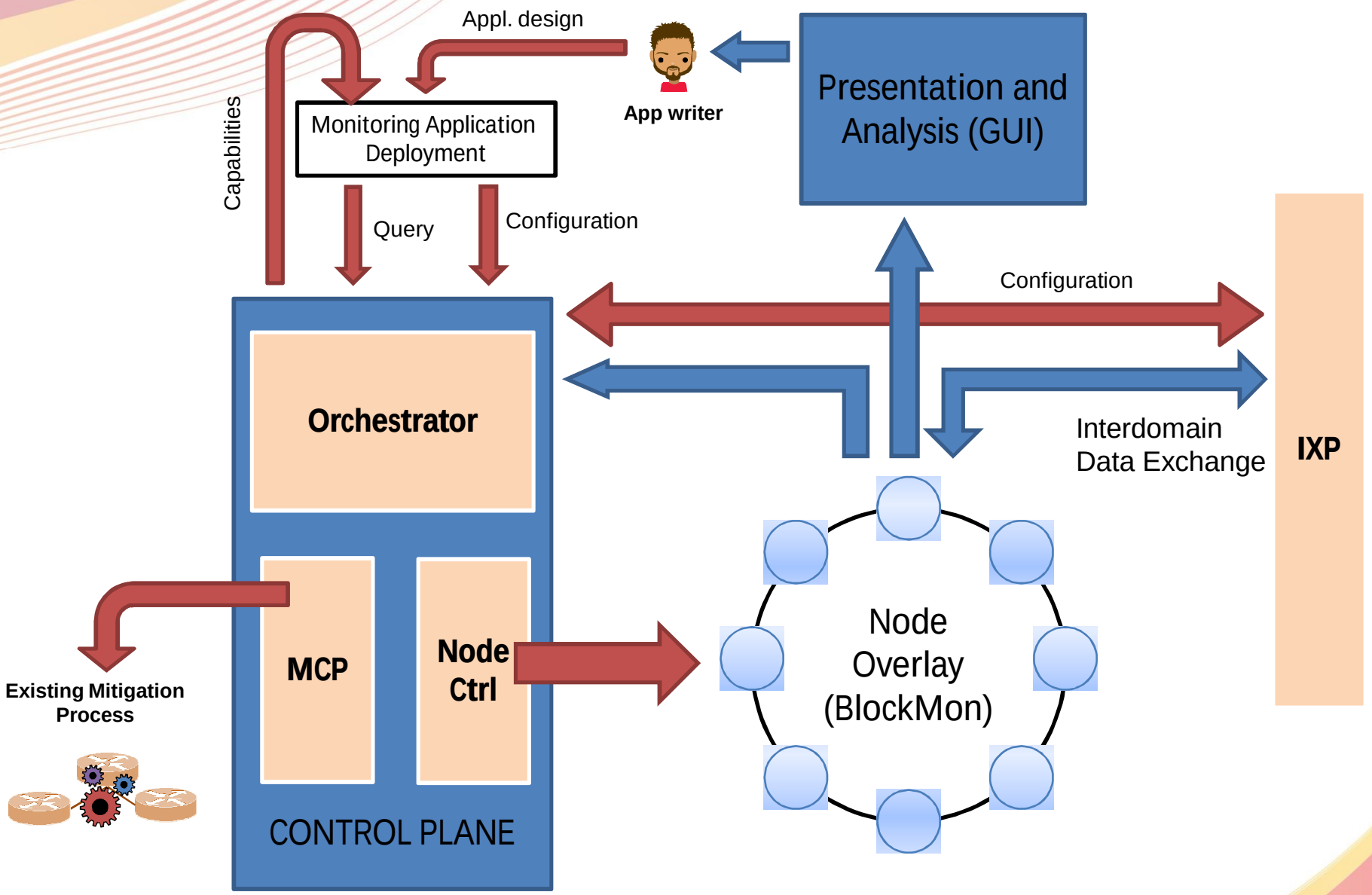
Selected Architectural Requirements

- ***Dynamic reconfiguration for scalability***: handle peak data volumes with high performance, grow/shrink/reconfigure with minimal delay
- ***Distributed infrastructure***: leverage multiple observation and processing points dealing with data distributed in space (thus need to cope with partial state information)
- Allow ***real-time analysis and mitigation*** as well as application of historical trends; deal with data distributed in time
- Support ***programmability*** of ***elementary processing tasks*** and ***dynamic composition*** of these primitives into more complex processing tasks.
- Allow ***decomposition*** of ***high-level monitoring application objectives*** to a pipeline of processing tasks
- Allow ***parallelization*** of multiple applications ***over the same monitoring infrastructure***
- ***Efficient export*** of measurement information (e.g., flow-level, compressed data structures)

DEMONS Architecture Elements

- **Nodes** provide traffic capture, data import, processing, and centralization of results.
- A **Node Controller (NC)** provides a central point for exchanging control information among nodes.
- An **Interdomain Exchange Point (IXP)** provides a well-known point of contact among domains, providing access control and data forwarding.
- A **Mitigation Control Point (MCP)** provides an interface to existing mitigation systems or incident handling workflow management.
- An **Orchestrator** manages the control-plane communications among the control points, providing a single interface for application development.
- A **graphical user interface** for each application accepts processed data from the Nodes

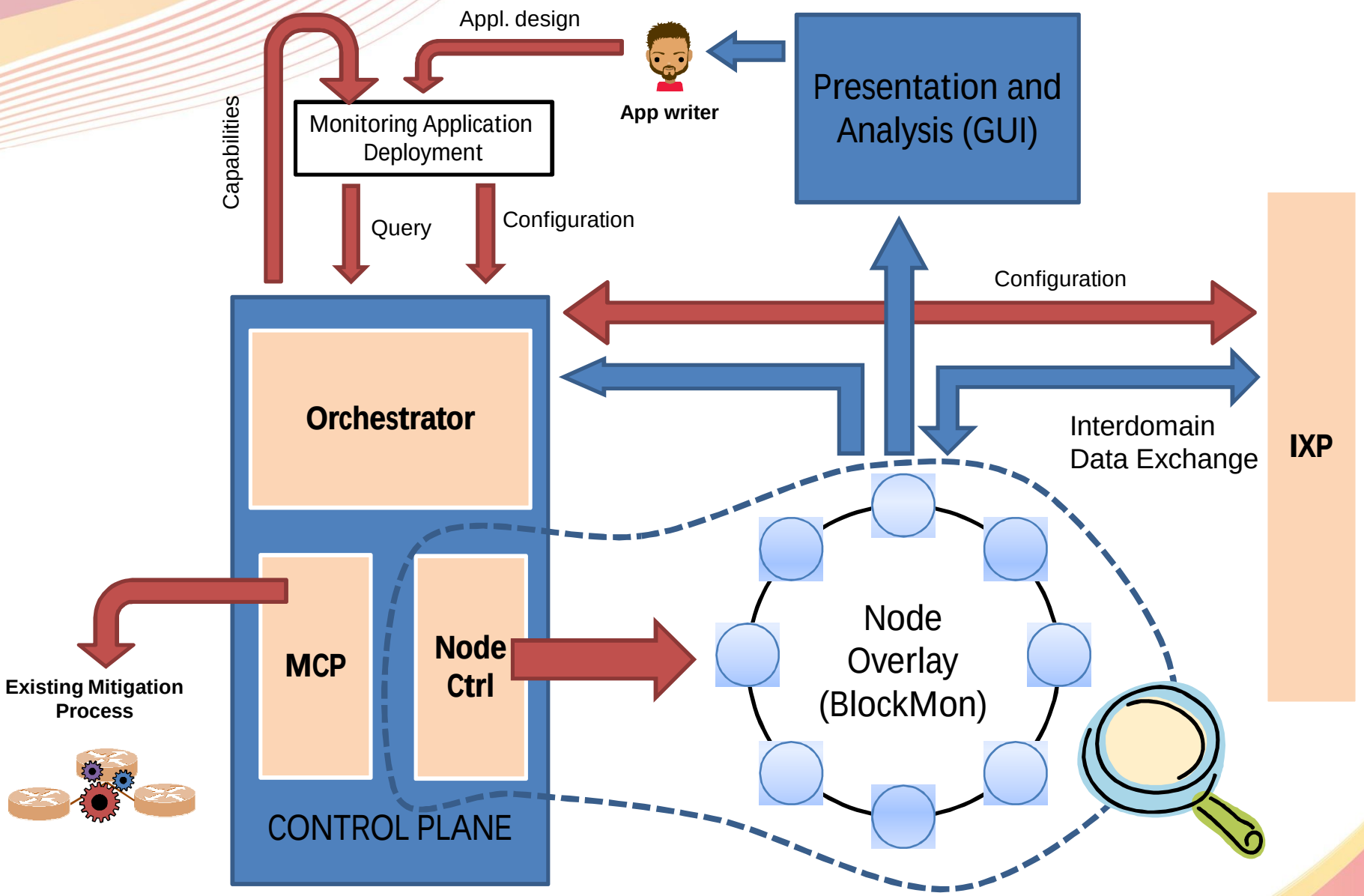
Intra-domain Architecture

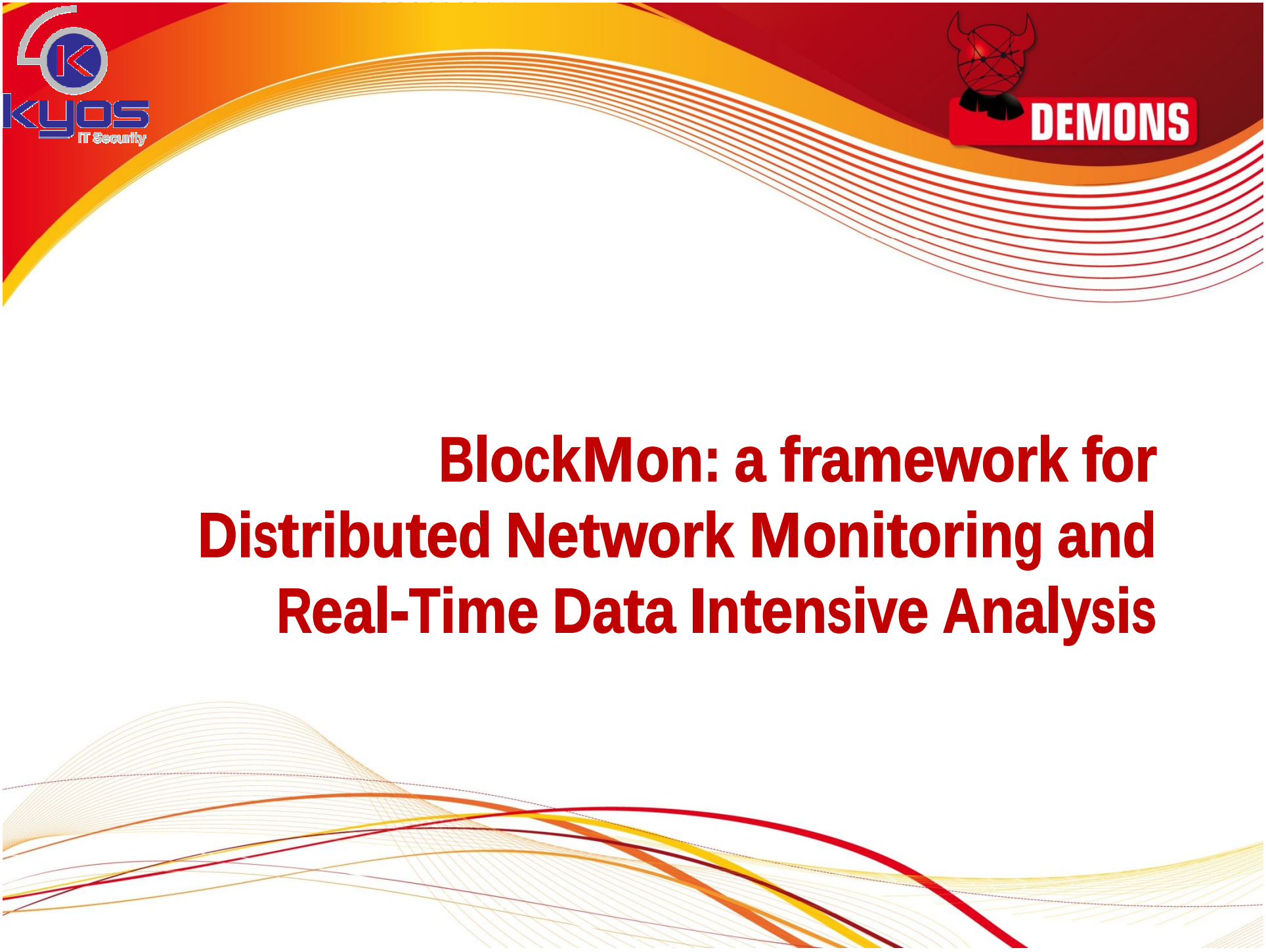


IPFIX in DEMONS

- Each Node may have an import interface (IPFIX Collecting Process) for accepting data via IPFIX from other Nodes or external exporters.
- Each Node may have an export interface (IPFIX Exporting Process) for sending data via IPFIX to other nodes, to a presentation system, or for handling by the MCP or IXP.

Intra-domain Architecture

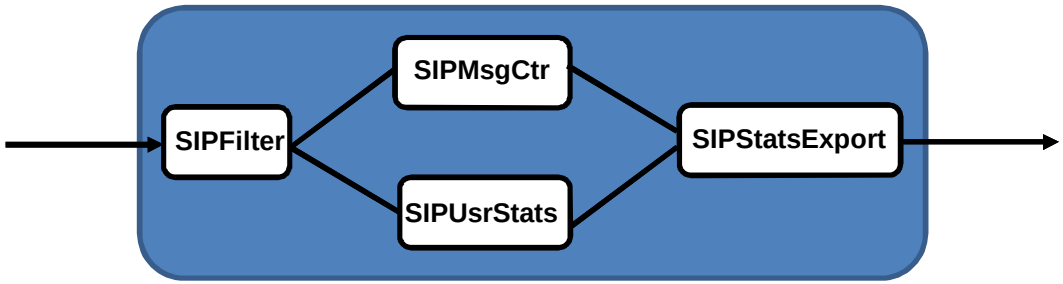




BlockMon: a framework for Distributed Network Monitoring and Real-Time Data Intensive Analysis

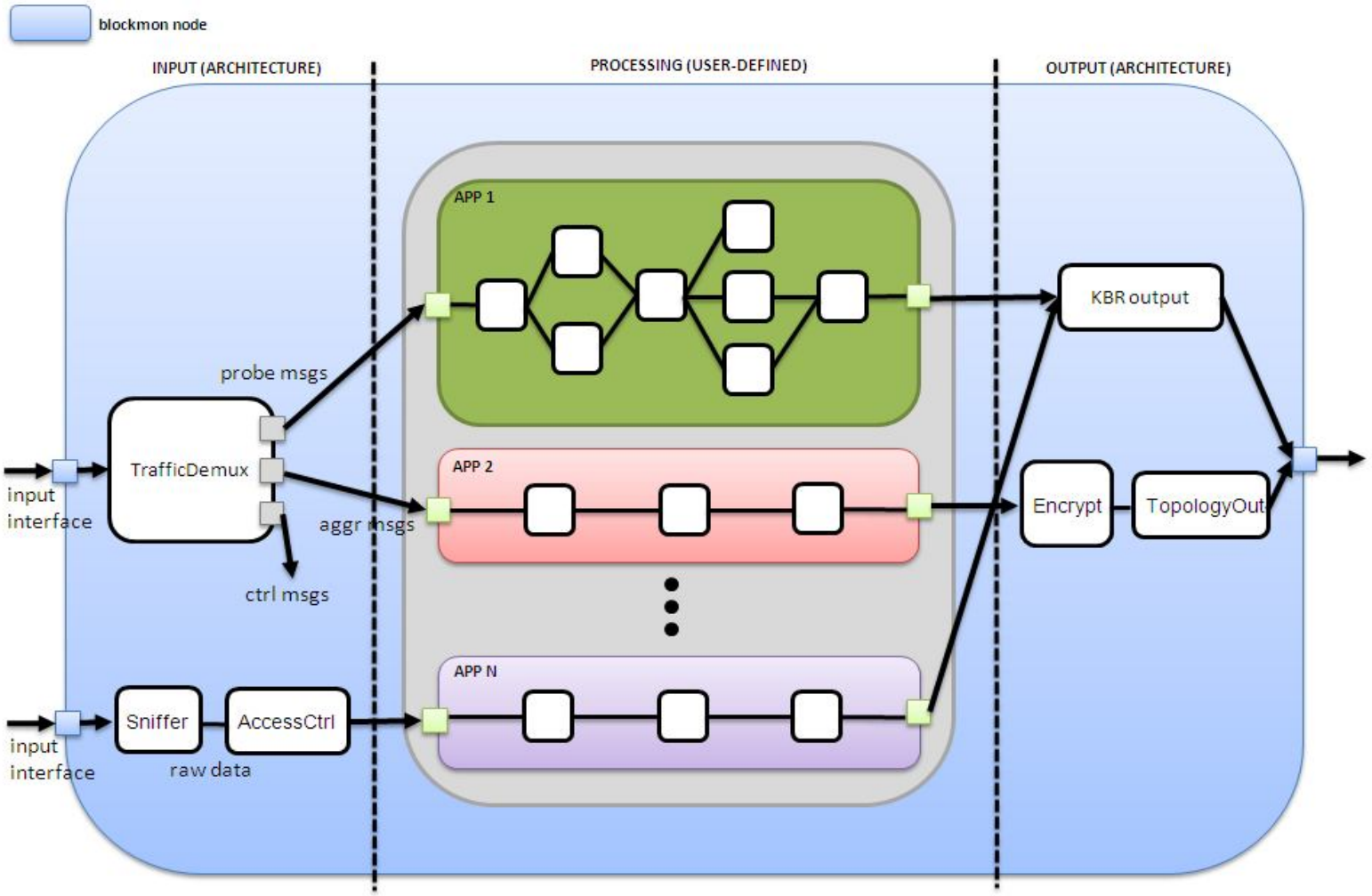
BlockMon's Node Architecture

- BlockMon composes monitoring logic from configurable *blocks*
  - A block is a small unit of processing, e.g. packet counting
- Blocks connect to each other through input and output *gates*
- Processing in a BlockMon node is done through a *composition*
  - A composition is a set of inter-connected blocks
  - See example below



Requirements addressed:
• Allow ***programmability*** of ***elementary processing tasks***
• Allow ***dynamic composition*** of elementary processing task into more complex processing tasks (***serialization***)

General Node Architecture

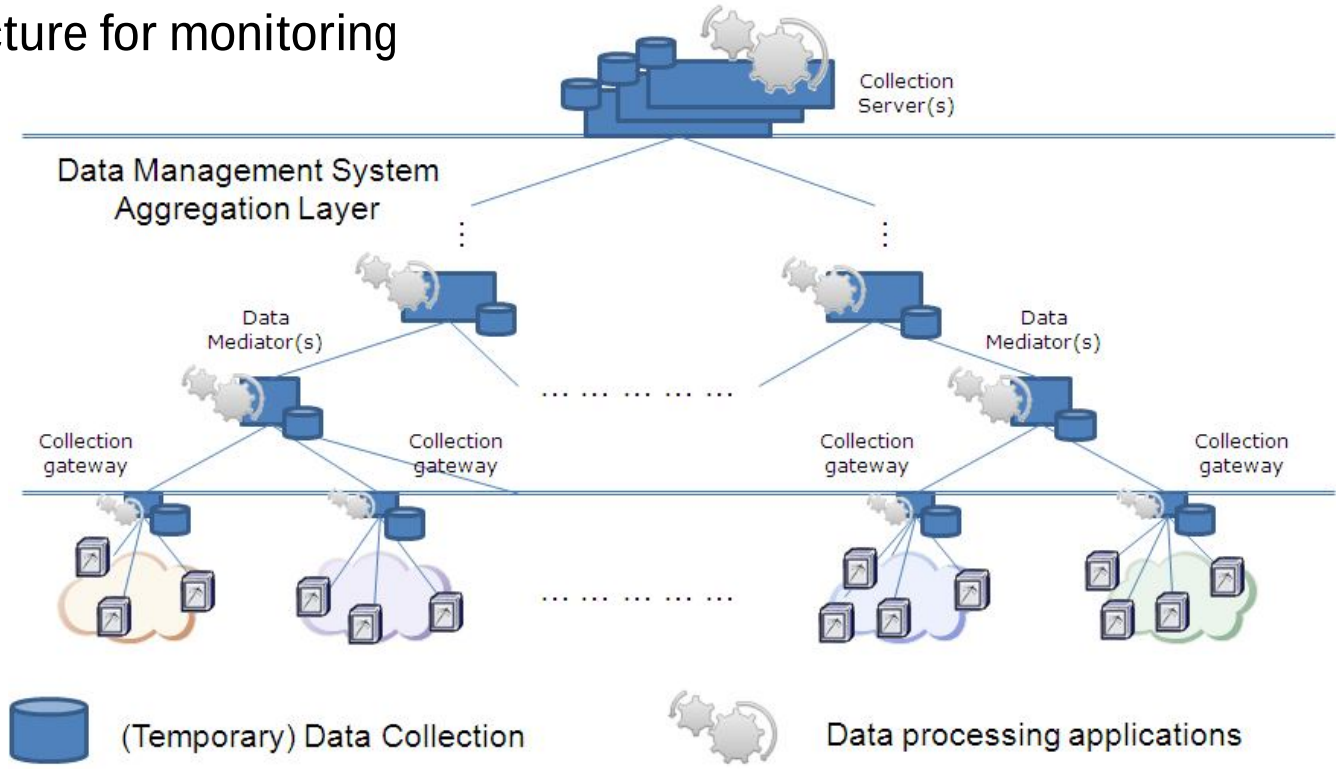


Requirements addressed:

- Allow ***parallelization*** of multiple applications ***over the same monitoring infrastructure***

Addressing scalability and distribution of data in space

- Data is distributed in space → distribute the infrastructure for monitoring
  - Process data locally as much as possible, aggregate and export



Requirements addressed:

• ***Be distributed in nature***: leverage multiple observation and processing points dealing with data distributed in space (thus need to cope with partial state information)

• Allow ***real-time analysis and mitigation*** (as opposed to historical analysis and no reaction): deal with data distributed in time

BlockMon Control Functionality

- Distributes configuration and composition to BlockMon nodes.
- Generates and dynamically reconfigures per-application topologies across a set of nodes
- Instantiates processing in each of the nodes of a topology
- Allows node management and maintenance
  - Monitors current nodes, retrieving current performance statistics to better allocate processing to nodes
- Dynamically scales depending on current traffic patterns

Interfaces in the DEMONS World: IXP, MCP, and Orchestrator

Interdomain Exchange Point (IXP)

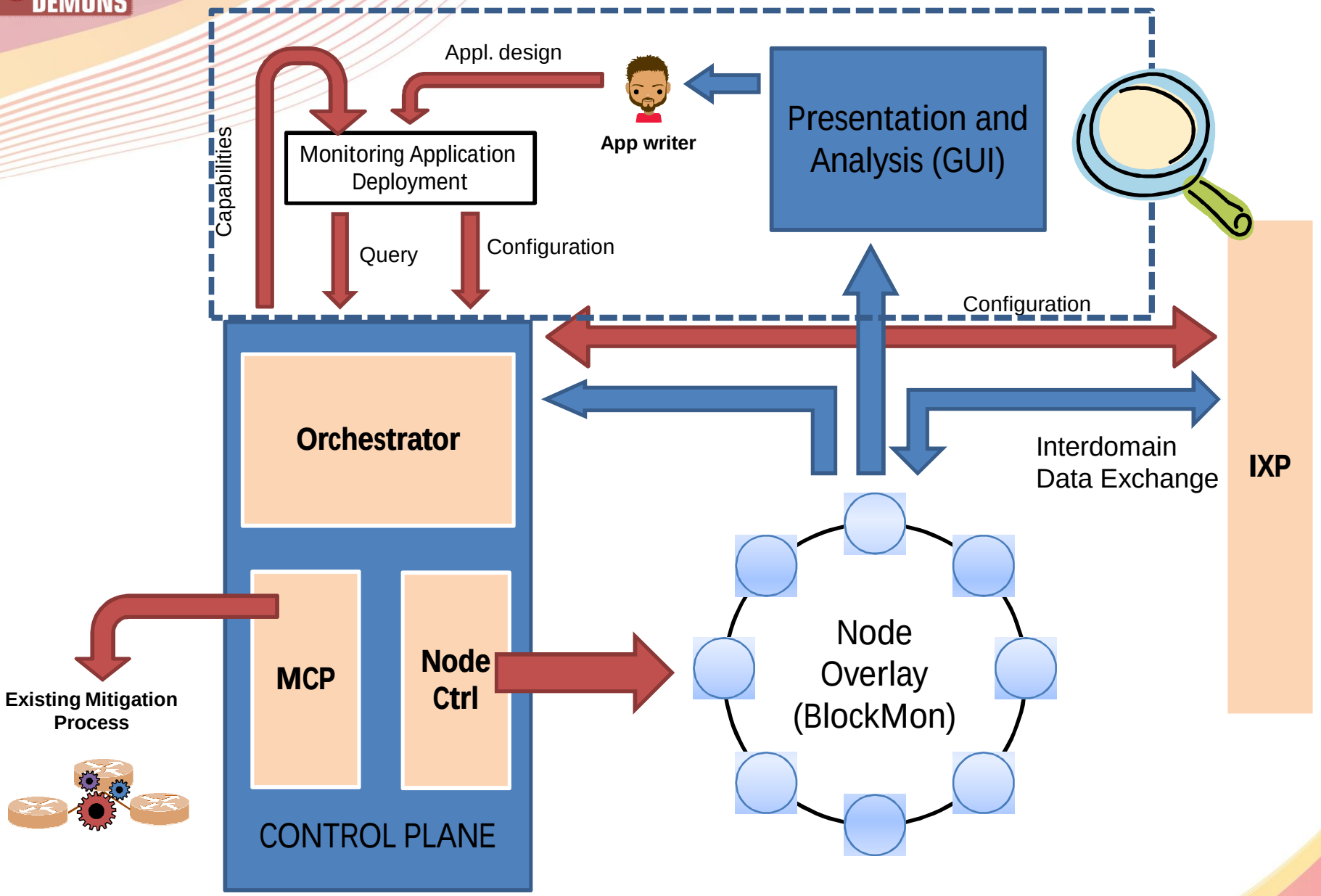
- Communication among domains must be coordinated at a well-known point for each domain
  - Access control, security policy, audit, etc.
- IXP mediates inter-domain communication
  - Buffers data for inter-domain measurements on non-sensitive information
- IXP forwards both data and control messages

Mitigation Control Point (MCP)

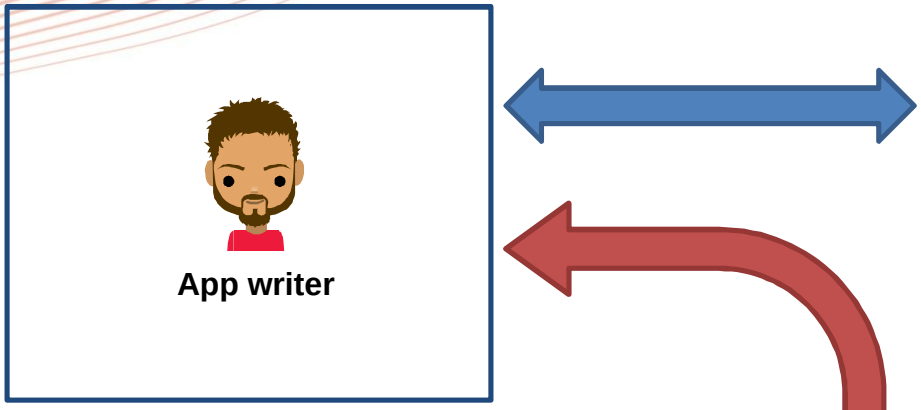
- Most operators have established procedures for network-level mitigation, and workflows/tools to support them.
- The MCP acts as an interface to these to allow flexible deployment of mitigation.
- MCP accepts data as well as control messages
  - Data from nodes indicating traffic to mitigate
  - Control from MCPs in other domains via IXP

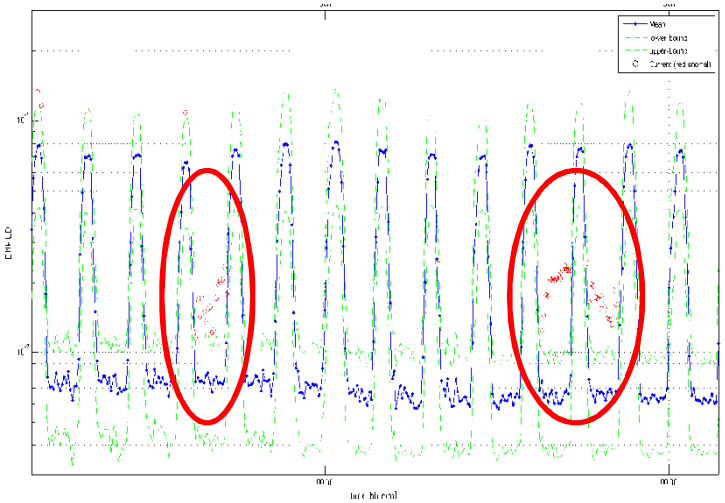
The application block

Intra-domain Architecture



Application Layer Interactions





1. Need A, B, C

2. Got A, B’

3. Push Appl.

x= OP1(A)
y= OP2(B’)
Result=OP3(x,y)

4. Config. Approval

5. Results

Orchestration

Authorisation and Access Control

The starting point: DEMONS Inheritance

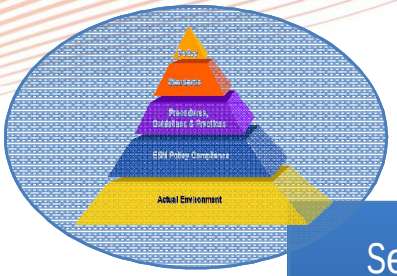
- Organization-Based Access Control (OrBAC)
  - One of the most mature and cited access control models
  - Provides several extensions related to DEMONS
  - Comes with a variety of tools for policies management
  - Supports ontologies
  - Supports policy-driven adaptation strategies (e.g., negotiation of precomputed mitigation strategies)
- Access Control & Authorisation Model
  - Specifically devised for privacy in network monitoring
  - Yet, it constitutes a general purpose framework
  - Fully based on ontologies & X.509 Attribute Certificates
  - Supports the specification of workflows for data transformations
  - Product of joint work between engineers & lawyers

Privacy by Design

- *Privacy by Design* reflects the concept whereby privacy and data protection compliance is designed into systems holding information right from the start
- Directive 95/46/EC requires that:

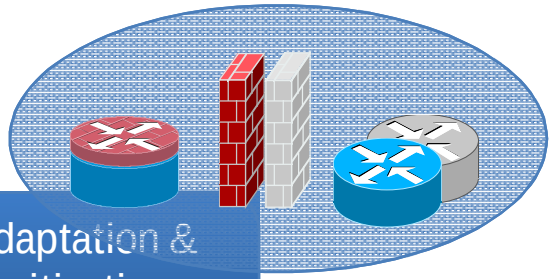
  …appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself…
- DEMONS aims at the higher degree of automation regarding the enhancement of applications with privacy-enhancing features already at their specification phase

Dynamic policy-based mitigation

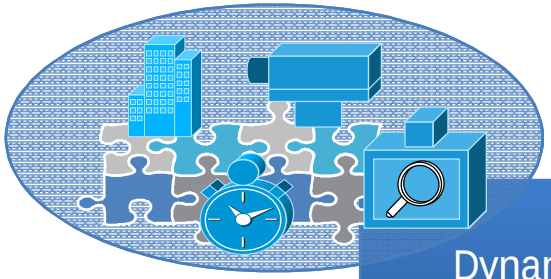


Security & privacy regulations

Policy



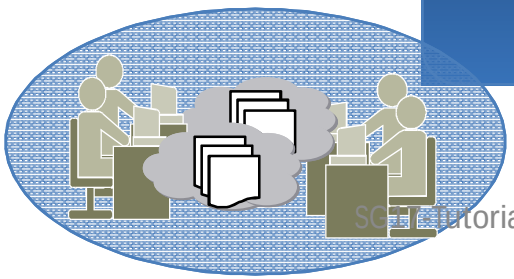
Adaptation & mitigation capabilities



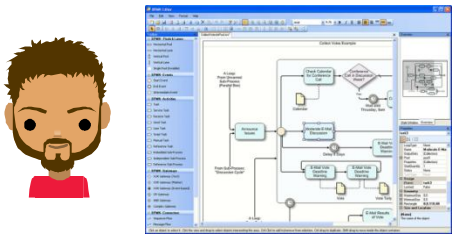
Dynamic contexts

Negotiation support

Delegation of capabilities

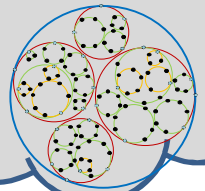


Overall approach



User Goals

Capabilities



DEMONS

Policies

<?xml version="1.0"?>
<rdf:RDF
xmlns:xsp=http://www.owl-ontologies.com/2005/08/07/xsp.owl#
... ...
... ...

- Goal decomposition
- Privacy-awareness
- Refinement

Executable Workflows

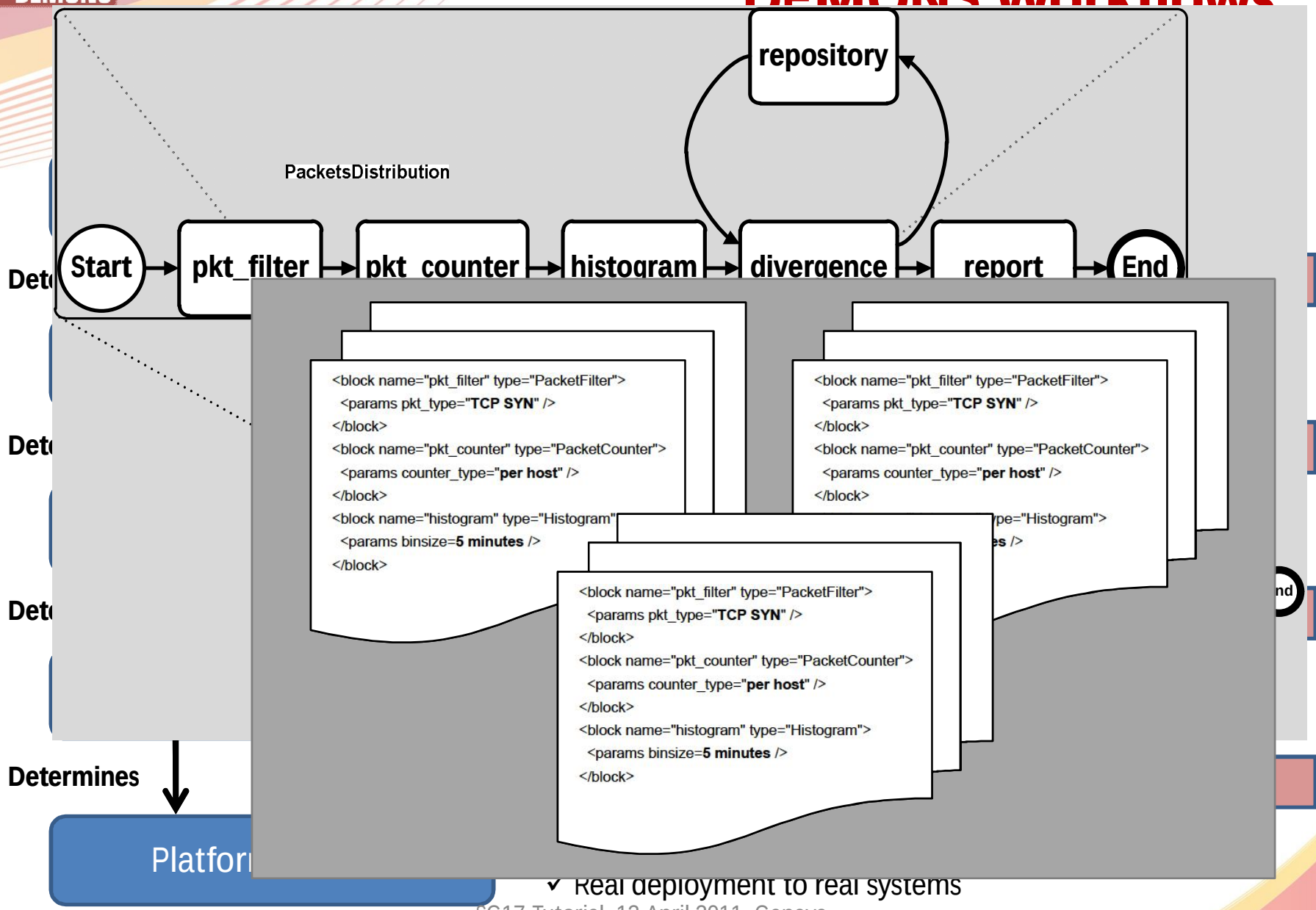
```
<workflow>
        <description>This workflow detects and mitigates botnets </description>
        <inputs>
                <input name= 'Traffic' data-type= 'IPFIX'/>
                <input name= 'StatADParameters' control-type= 'StatADParameters' value =
        'TCP SYN, per host, 5    minutes, 2 weeks, 0.95, kullback-leibler'/>
                <input name= 'FastFluxParameters' control-type = 'FastFluxParameters' value
= '...' />
                <input name= 'EvaluationParameters' control-type = 'EvaluationParameters'
        value = '...' />
                <input name= 'MitigationParameters' control-type = 'MitigationParameters'
        value = '...' />
        </inputs>
        <outputs>
                <output type= 'DetectMitigateBotnetsReport'/>
        </outputs>
        <sequence>
                <flow>
                        <sequence>
                                <invoke component =
'monitorPacketsDistributionComponent_1'...>
                                        <inputs Traffic fromComponent= 'probe_1'/>
                                        <outputs StatAdAlarm, StatAdReport    toComponent=

'EvaluationOfDetectionResultsComponent_1'/>
                                </invoke>
                                <initialize component=
'monitorPacketsDistributionComponent_1' with=
        'StatADParameters'/>
                                <run component=
'monitorPacketsDistributionComponent_1'/>
                        </sequence>
                        <sequence>
                                <invoke name= 'FastFluxDetectionComponent_1'...>
                                        <inputs Traffic fromComponent= 'probe_1'/>
                                        <outputs FastFluxAlarm, FastFluxReport
toComponent=
        'EvaluationOfDetectionResultsComponent_1'/>
                                </invoke>
                                <initialize>...
                                <run>...
                        </sequence>
```

Overall approach

- Introduce privacy-awareness to Operations and Workflows
  - Blocks development
  - Blocks Composition
  - Operator-level Workflow
  - DEMONS-level Workflow
- Include mitigation strategies in the Workflows
  - By means of dynamic security policies
  - Mitigation actions: Operations
  - Triggered as a result of *alerts*, represented by contextual parameters activation
- Approach: policy-based, semantics-aware, model-driven

DEMONS Workflows:



- ✓ Real deployment to real systems

Privacy-enhancement: Blocks & Compositions

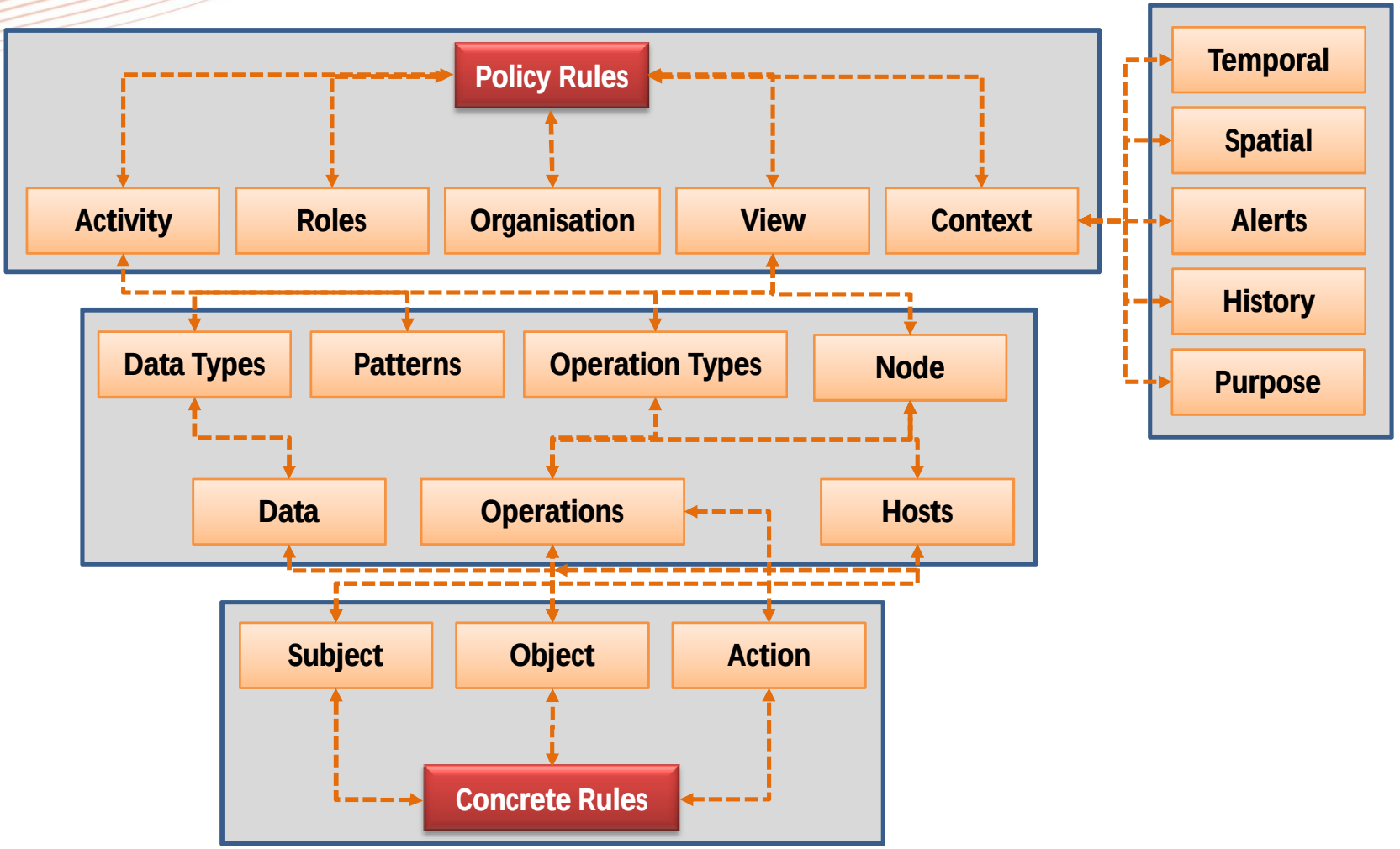
- Block development
  - Each Block represents an Operation
    - Abstracted as a DEMONS Service
    - With specific semantics (e.g., a “PacketCounter”)
  - WSDL-like description, enhanced with metadata related with security & privacy
    - e.g., user roles allowed to execute the Block
- Composition
  - Higher level semantic Operation
  - Inherits features from its Blocks
  - Description enhanced with security & privacy provisions
  - Need to check various types of accesses

Privacy-enhancement: Workflows validation criteria

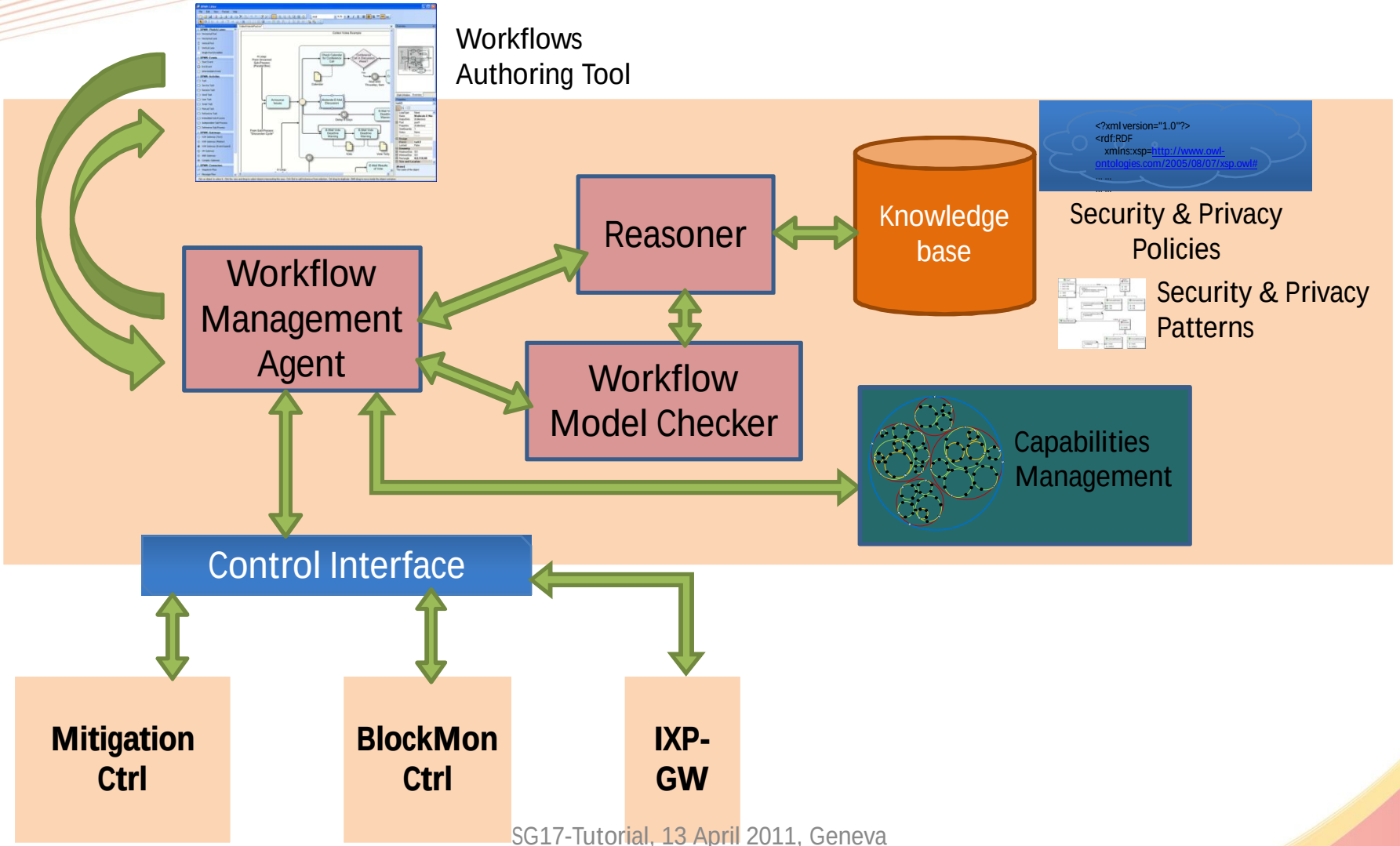
- Purpose compliance
  - A distance-based approach comparing the user-declared purpose with the defined Operations' "sum"
- Access constraints
  - User → Operation
  - User → Data
  - Operation → Operation
  - Operation → Data
- Access constraints++
  - Multi level verification
  - Path-based verification
- Inter-domain case
  - Verification at the attachment points
  - Negotiation of access parameters (e.g., ontological role mapping)

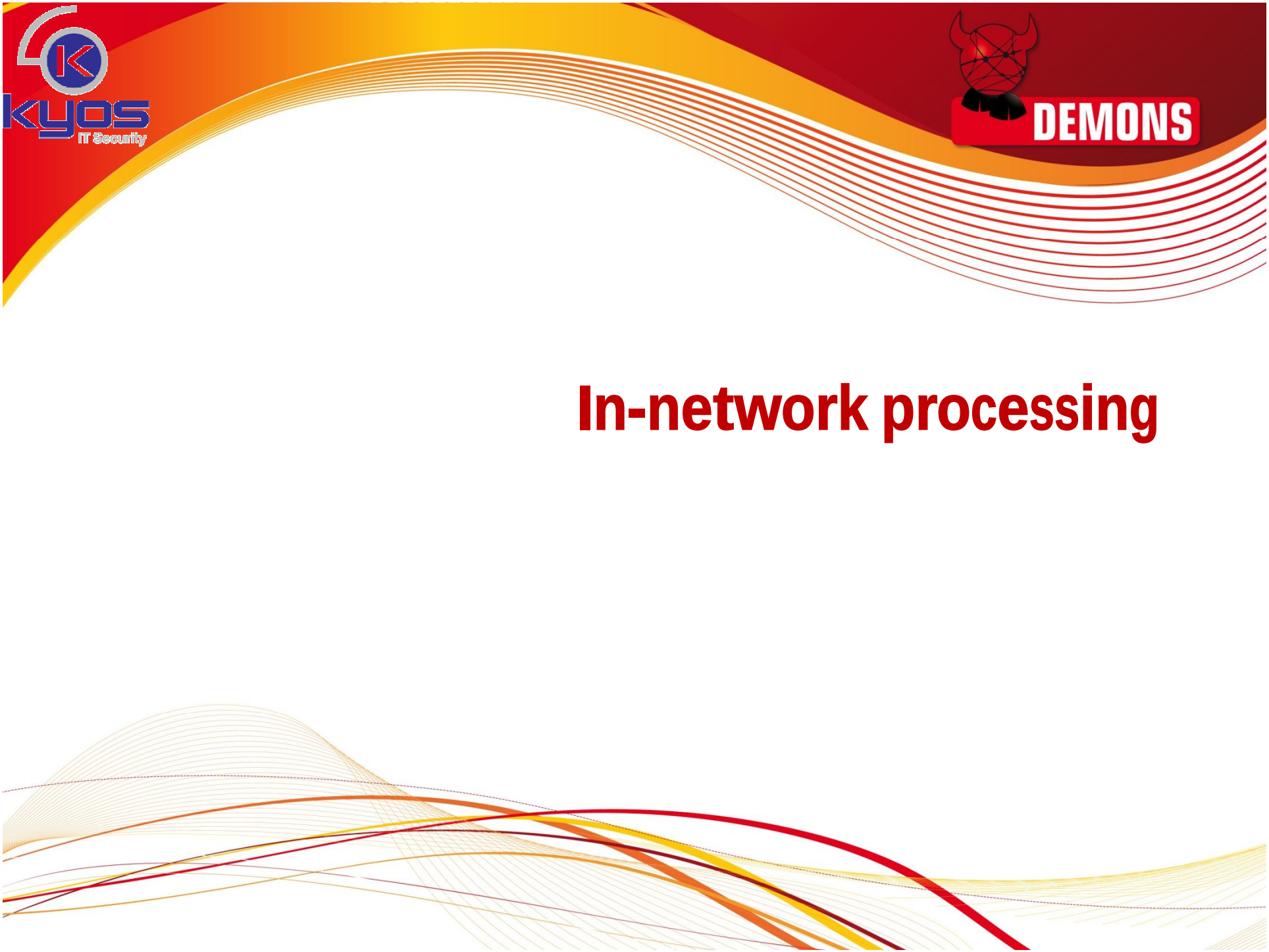
DEMONS

Policy model



DEMONS Orchestrator

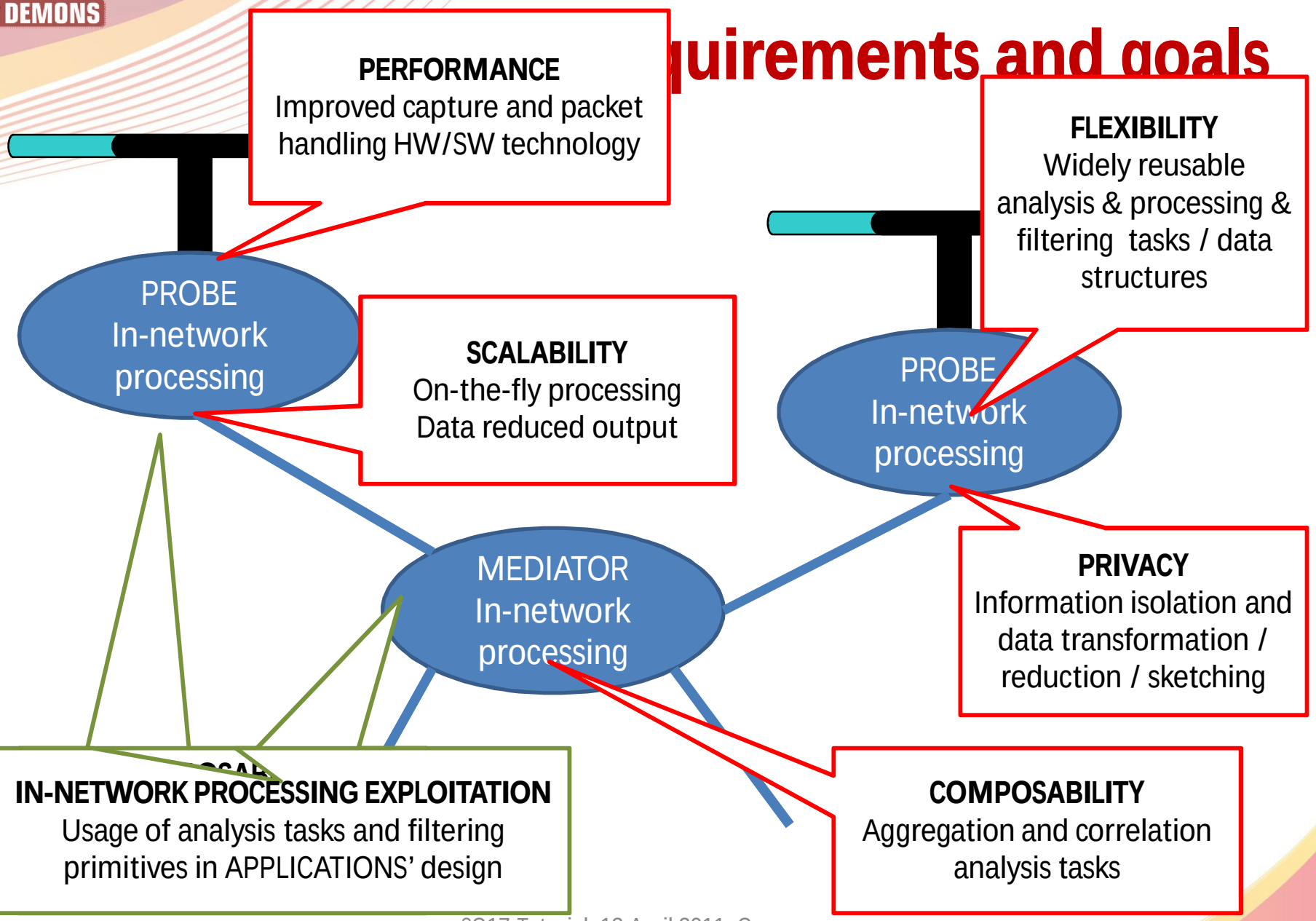


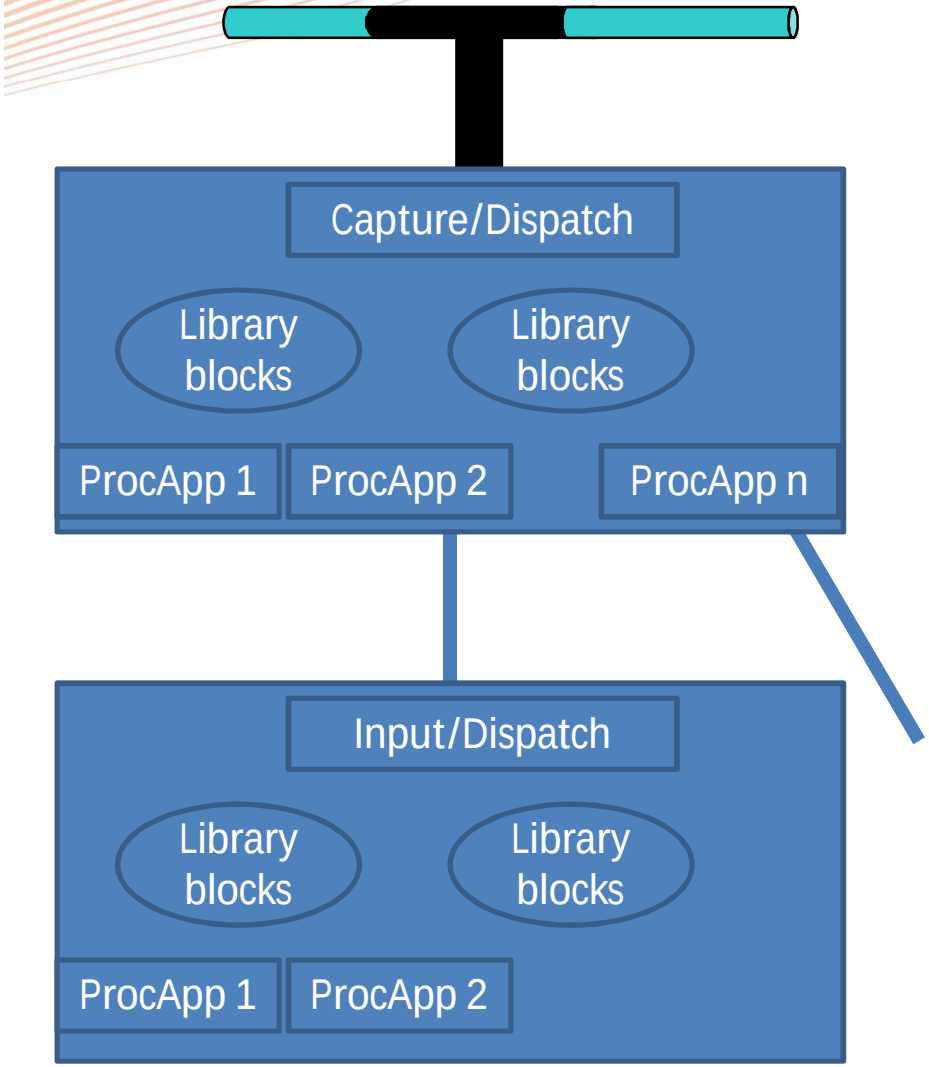


In-network processing

DEMONS

quirements and goals





Approach

- Processing
  - Filtering
  - Metering
  - Isolate “interesting” events
  - Aggregate/compare
  - …
- Tools
  - Matching/filtering/parsing
  - High performance analysis
    - Bloom filters & Extensions
    - Extending PRISM inheritance

Tasks involved

- Analysis primitives and aggregation issues
- SW acceleration
- HW acceleration

Threat detection and defense solutions

COLLABORATION

- Goals
  - enable/exploit collaboration between monitoring instances
  - change/evolve legacy instances as needed to fit in [take advantage from] a collaborative framework
  - focus not (necessarily) on new algorithms, but on their application/adaptation to a collaborative/decentralized framework

Collaboration

- Multiple forms of collaboration: between …
  - multiple ISPs [inter-domain]
  - different sensors
    - gather and reuse inputs from legacy systems like commercial IDS/IPS, spam-filters… [intra-domain]
  - monitoring probes
    - decentralized monitoring [intra-domain]

Target monitoring applications

- Botnet detection
  - centralized C&C → by fast-flux detection
  - p2p C&C → by analysis of collaboration graphs
- DDoS detection and mitigation
- VoIP threats detection
- Collaborative intrusion detection
- Statistical-based anomaly detection

List of monitoring applications

monitoring application	inter-domain coll. between ISPs	coll. between different sensors	coll. between monitor probes
Botnet - domain-flux detection	✔✔✔		
Botnet – collaboration graph	✔✔✔	✔	
Statistical Anomaly-Detection	✔✔		✔✔
Collaborative IDS – alarm scoring	✔	✔✔✔	
Collaborative IDS – decentralized filters			✔✔✔
VoIP trustworthiness	✔		✔✔✔
DDoS detection and mitigation ??	✔✔		??

Dissemination and Standardisation

Project website

- www.fp7-demons.eu and www.fp7-demons.org are operational with the status of the project.

Dissemination: publications

General awareness

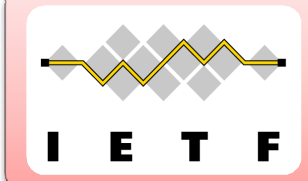
- Project factsheet
- Project presentation
- Press release

Available on the website

Technical publications

- 8 workshop presentations
- 3 conference papers
- 2 journal publications

Standardization



Contributions to IPFIX

- http://tools.ietf.org/html/rfc6046 (published)
- http://tools.ietf.org/html/draft-ietf-ipfix-anon-06 (contributed and in discussions)
- http://tools.ietf.org/id/draft-trammell-ipfix-a9n-01.txt (draft)
- http://tools.ietf.org/id/draft-claise-ipfix-mediation-protocol-02.txt (draft)

Cooperation with INS ISG

- Contact with INS ISG
- Working on defining a new activity within the ISG

Liasion with SG-17

- First contact done
- Studying how to let SG-17 participate into the project.

Featured Event

DEMONS hosted the **IPFIX Interoperability event** (http://fp7-demons.eu/?p=164) in Prague during 24-25 Mar. 2011

DEMONS: so young and so mature…

- DEMONS targets to solve the limitations of today's monitoring systems in order to enhance the trustworthiness of the Internet
  - Providing a paradigm shift: ***from data-gathering devices to collaborative computing and filtering devices with privacy built-in by design***
- The project is working at full speed
  - Deep analysis of SoA
  - First release of use cases and requirements
  - Dissemination (e.g., 2 journal publications), standardization (e.g., IETF, ETSI, ITU)
  - Preliminary architectural vision
- Several technological contributions already outlined
  - Authorization and access control models
  - In-network traffic processing technologies
  - Privacy-enhancing cooperation solutions
  - Decentralized and cooperative threat detection techniques

Thank you for your interest in DEMONS

Please visit www.fp7-demons.eu for more information on the project

For background information on privacy, visit

www.fp7-prism.eu