Toward Real-time Network-wide Cyber Situational Awareness

Mini-conference NOMS 2018,

April 27, 2018,

Taipei, Taiwan

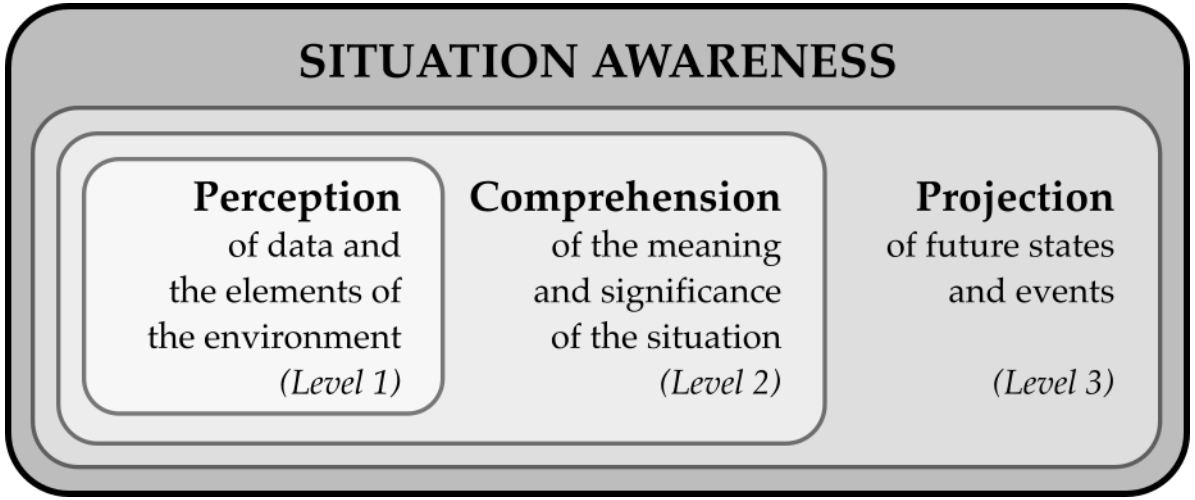
Tomas Jirsik, Pavel Celeda

Institute of Computer Science & Faculty of Informatics,
Masaryk University, Czech Republic

Cyber Situational Awareness

Network-wide Cyber Situational Awareness

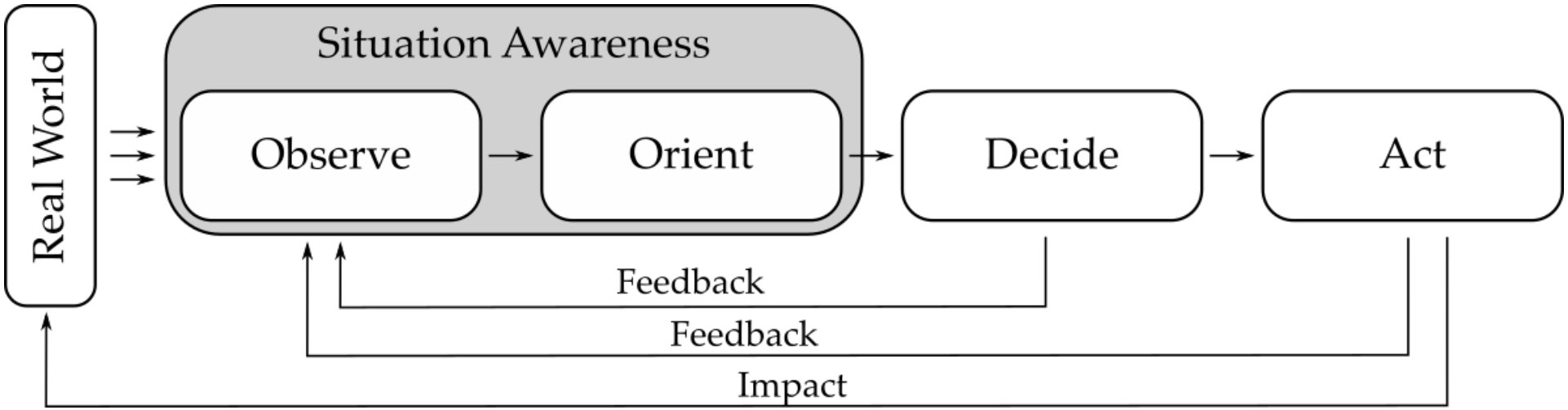
Perception of the elements in the computer network within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future. (Endsley 1998)



Specifics

- **Cyber environment** – no borders, scale free
- **Perception** – only by sensors
- **Performance** – small resources to harm, huge resources to protect
- **Attackers**– takes the advantage

Cyber Situational Awareness



Motivation

Data overload, meaning underload

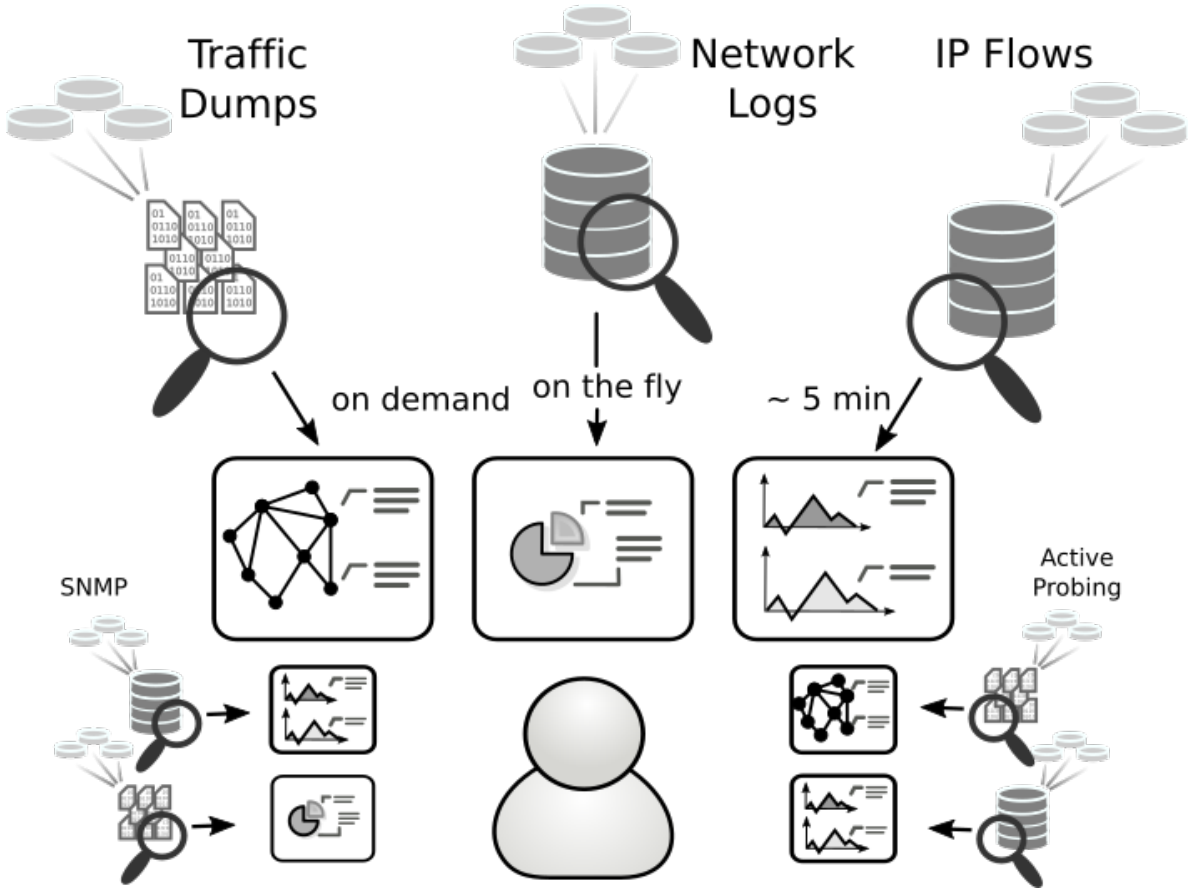
- An operator is overwhelmed with a raw data
- Big data in computer networks

Reaction speed

- Automated attacking tools vs human defender
- Speed of events
- Speed of processing

Heterogeneous Tools

- Various tools for different network data
- Both for data collection, analysis and visualization
- Performance is the issue



Requirements

Performance

- A framework should be able to process and analyze **large volumes of the data at high speeds**.

Universality

- A framework should be able to gather and process **data from various data sources**.

Context

- A framework should be able to offer **complete information including context** relevant to the information instead overwhelming a user with a flood of raw data.

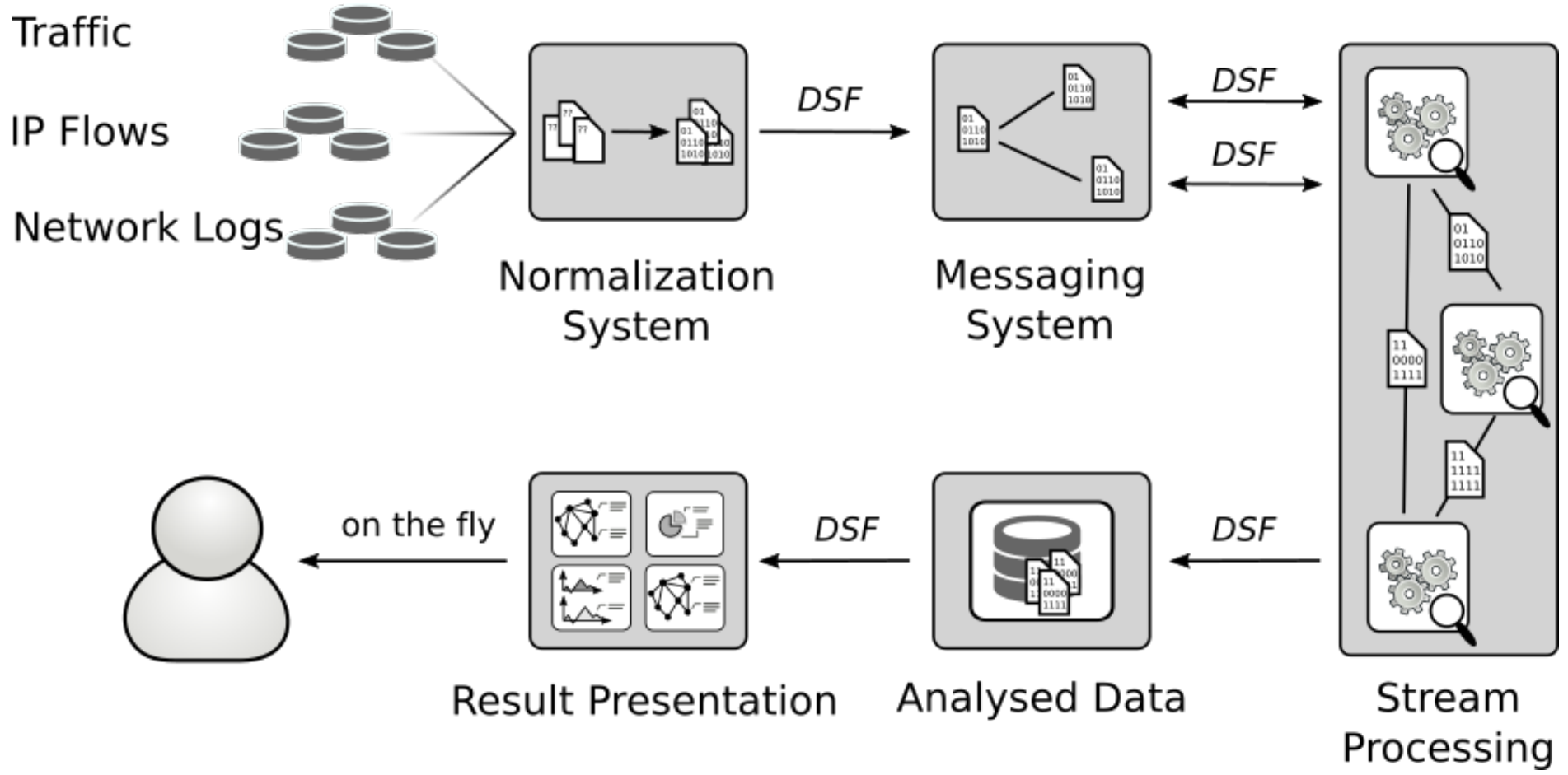
Dynamic Level of Detail

- A framework should be able to provide a dynamic level of detail both **in time and information domain**.

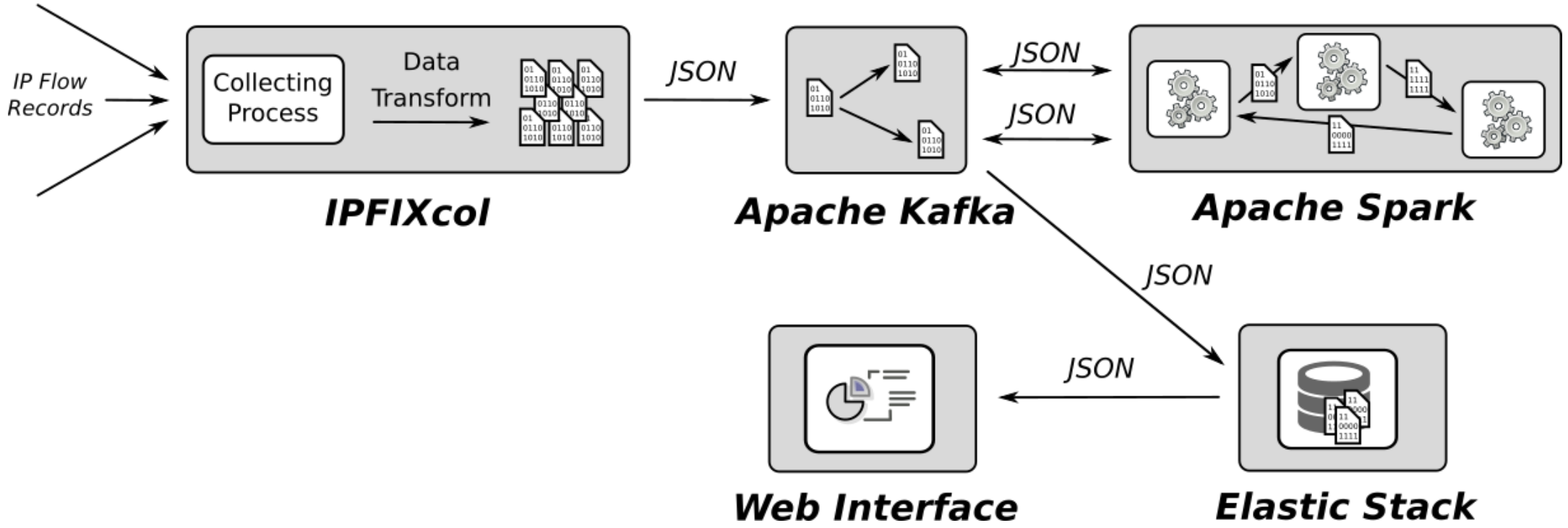
Reaction Time

- A framework **should minimize the tim**e needed for analysis to increase the speed of reaction.

Framework for Real-Time Cyber Situational Awareness



Stream4Flow: Prototype Implementation



Stream4Flow: Prototype Implementation

Discussion

Performance

- Scalability and throughput
- Data streams
- Distributed computing

Universality

- Normalization
- Data Message Bus

Dynamic Level of Detail

- High granularity in orders of seconds
- Map-reduce principle for host monitoring

Context

- Universality and performance enables context
- Correlation of events

Reaction Time

- On-the-fly processing

Further Remarks

- High granularity modifies data
- Deduplication

QUESTIONS?

THANKS FOR YOUR ATTENTION!

https://csirt.muni.cz

@csirtmu

Tomas Jirsik

jirsik@ics.muni.cz

CSIRT-MU