Big Data & Machine Learning for network security: approaches and benchmarks

Antonio Lioy (moderator)

< antonio.lioy@polito.it >

Politecnico di Torino

ICT-2018 networking session

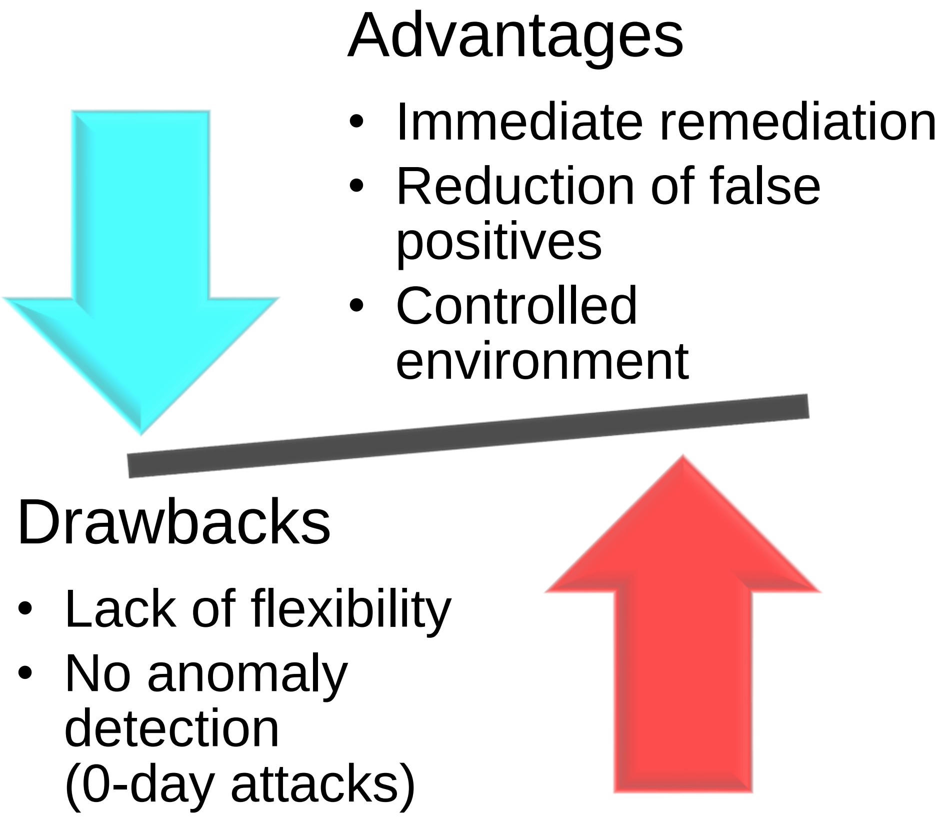
Vienna (Austria)

December 5th, 2018

Projects & speakers

- **SHIELD: ecosystem of on-demand virtualized security functions with (1) trust and integrity attestation of the physical infrastructure, and (2) central ML-based engine for attack detection and remediation**
  - **Bernat Gaston,** PhD, director of the Big Data and ML department in Fundació I2CAT, Barcelona
- **PROTECTIVE: evolve cyber situational awareness into effective ready-to- use security management solutions for CSIRTs and provide threat intelligence sharing capabilities**
  - **Maciej Miłostan**, is a security analyst in Poznań Supercomputing and Networking Center (PSNC)
- **C3ISP: data sharing and analytics for cyber threat information mgmt in a collaborative and confidential env**
  - **Andreas Alexiou**, International R&D Partnerships Lead at Digital Catapult; his background is in technology innovation

Rule-based systems vs ML approaches



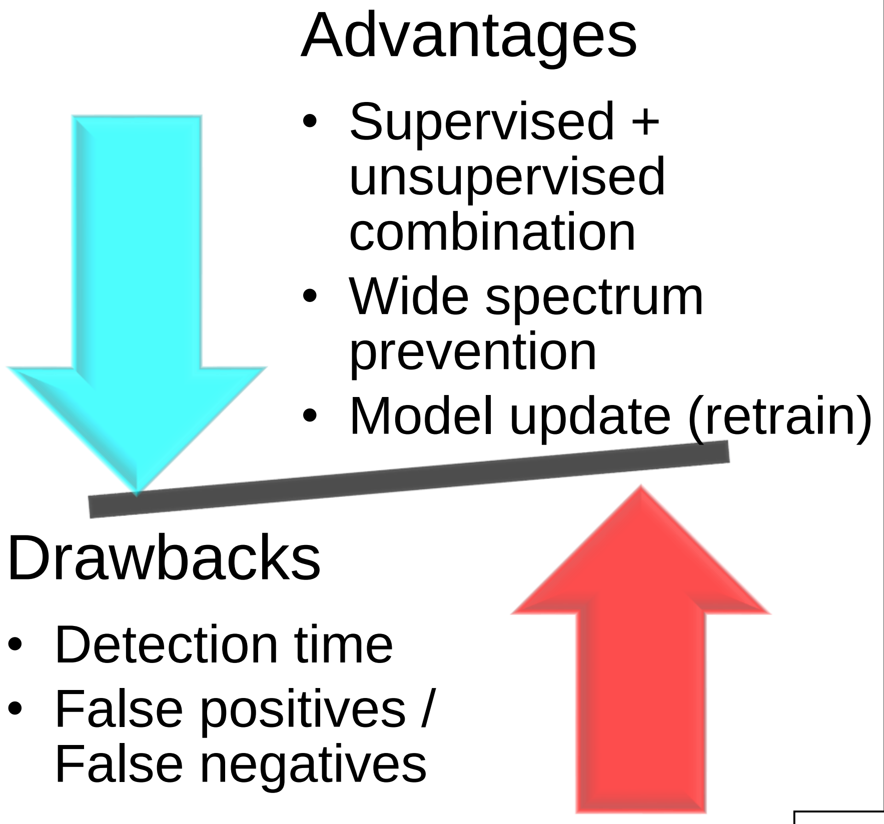
Rule-based systems

Advantages

- Immediate remediation
- Reduction of false positives
- Controlled environment

Drawbacks

- Lack of flexibility
- No anomaly detection (0-day attacks)



ML approaches

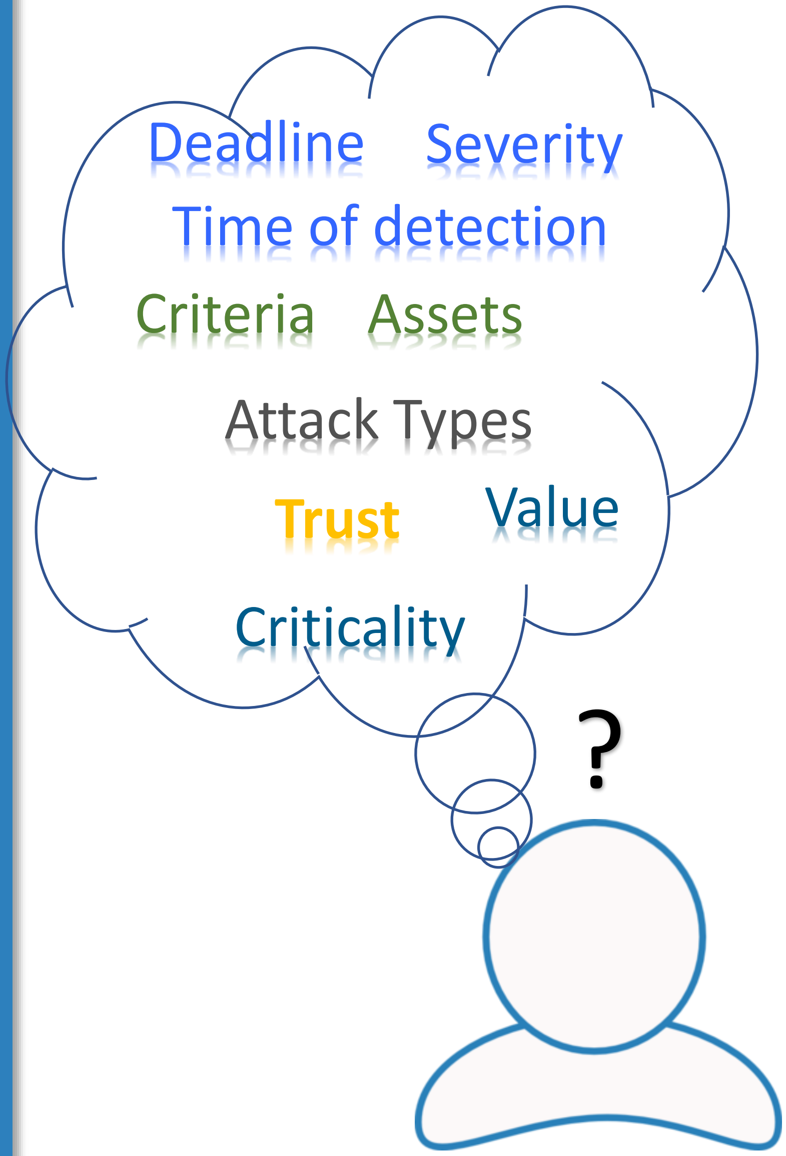
Advantages

- Supervised + unsupervised combination
- Wide spectrum prevention
- Model update (retrain)

Drawbacks

- Detection time
- False positives / False negatives

Prioritisation / Preference Learning



Deadline Severity

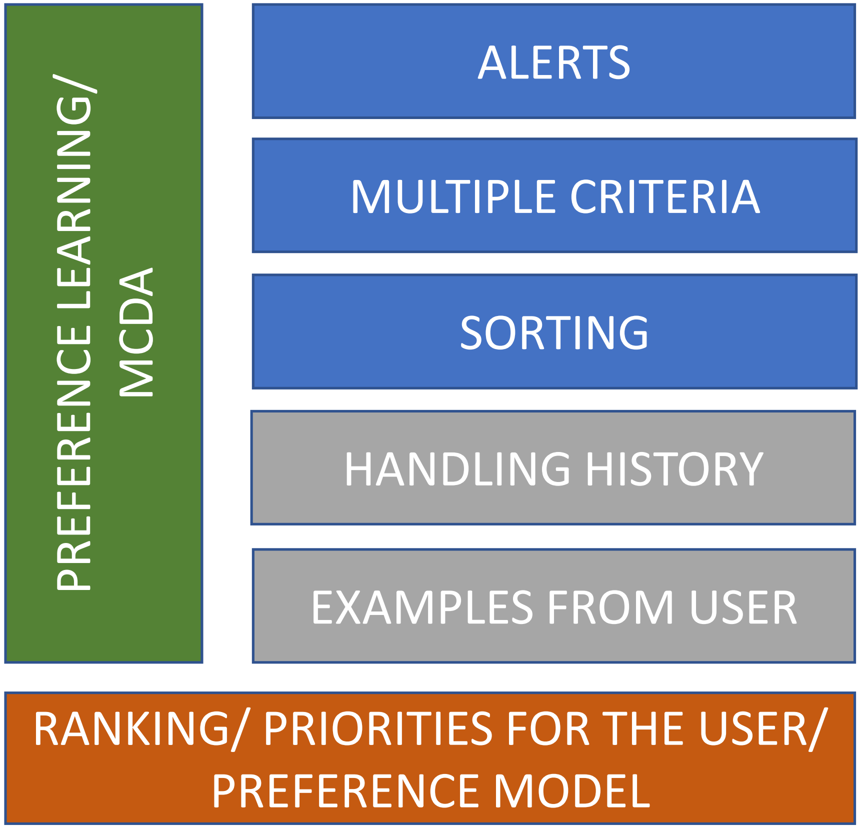
Time of detection

Criteria Assets

Attack Types

Trust Value

Criticality



PREFERENCE LEARNING/ MCDA

ALERTS

MULTIPLE CRITERIA

SORTING

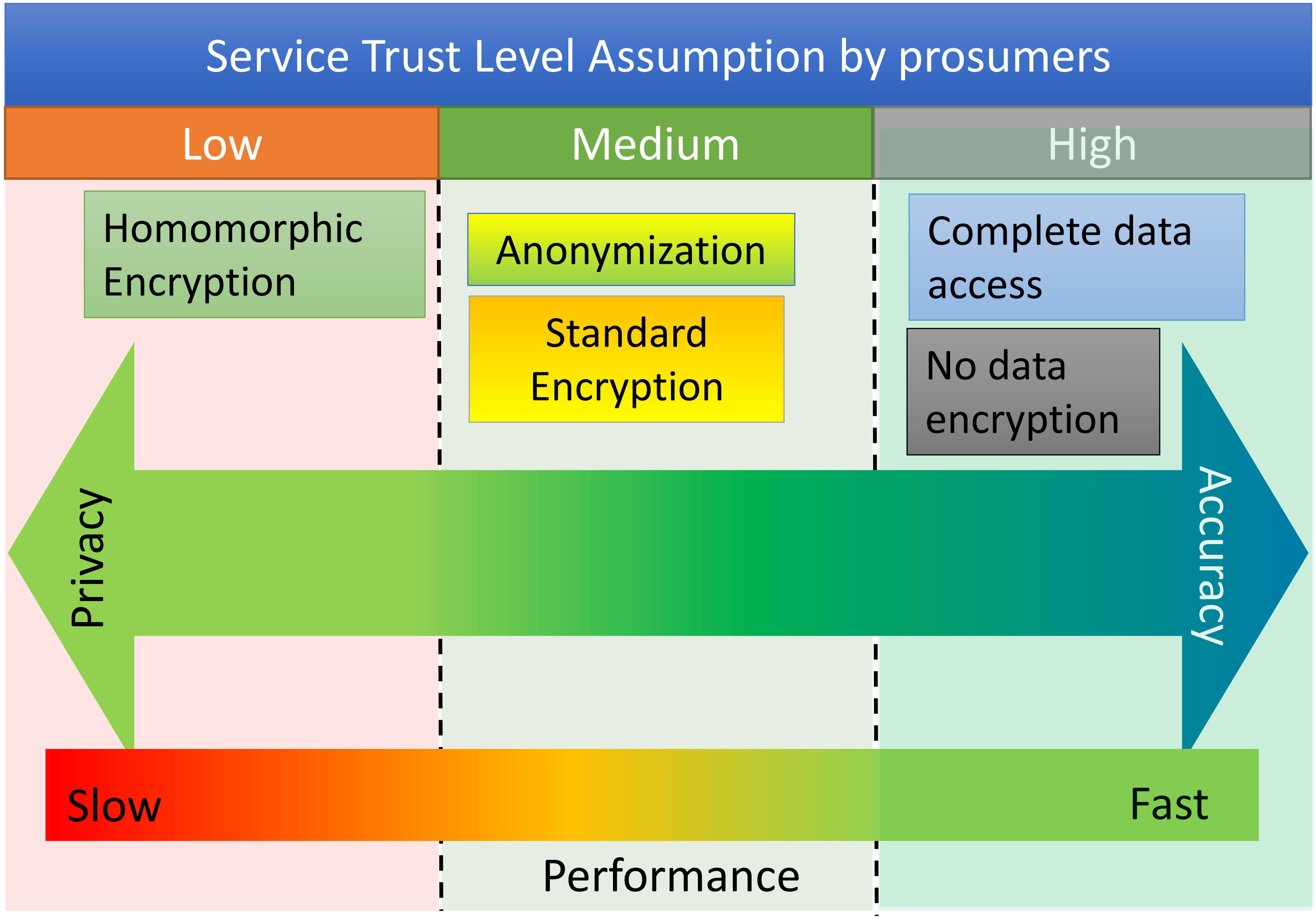
HANDLING HISTORY

EXAMPLES FROM USER

RANKING/ PRIORITIES FOR THE USER/ PREFERENCE MODEL

A dash board for trade-off between accuracy and privacy in analytics

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection



Big Data approaches to cybersecurity

SHIELD

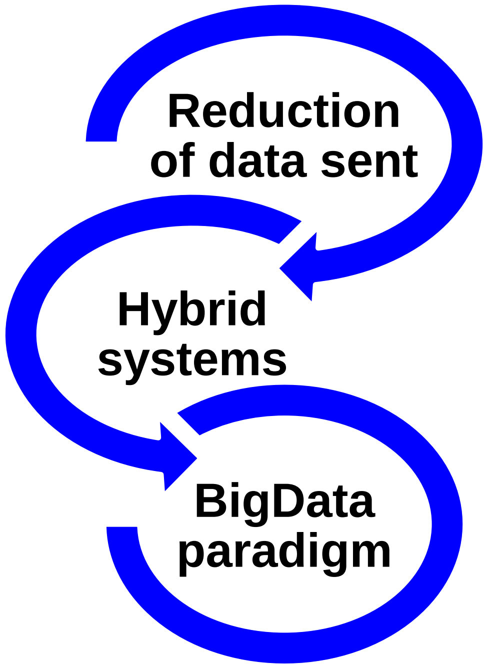
Centralized vs decentralized

Centralized	Decentralized
Holistic view of the system	Fast reaction
Heterogeneous data analysis	No extra traffic

More informed decisions

Faster decisions

From decentralized to centralized

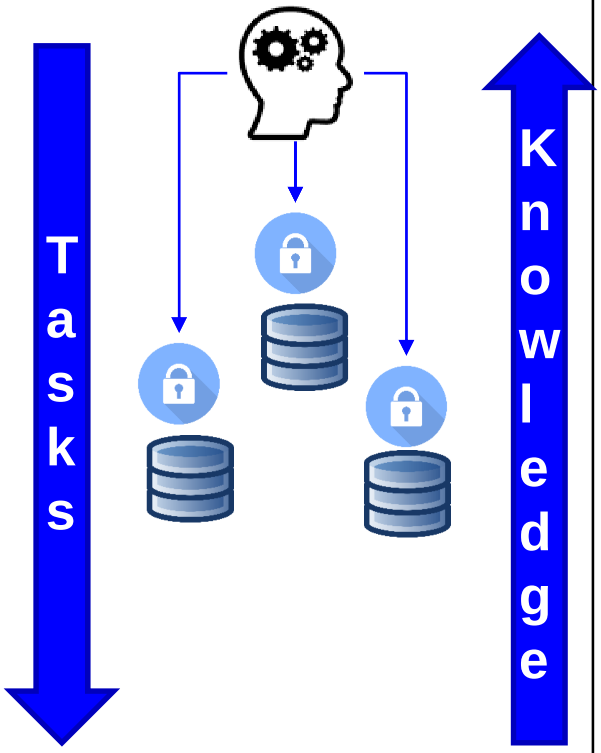


Reduction of data sent

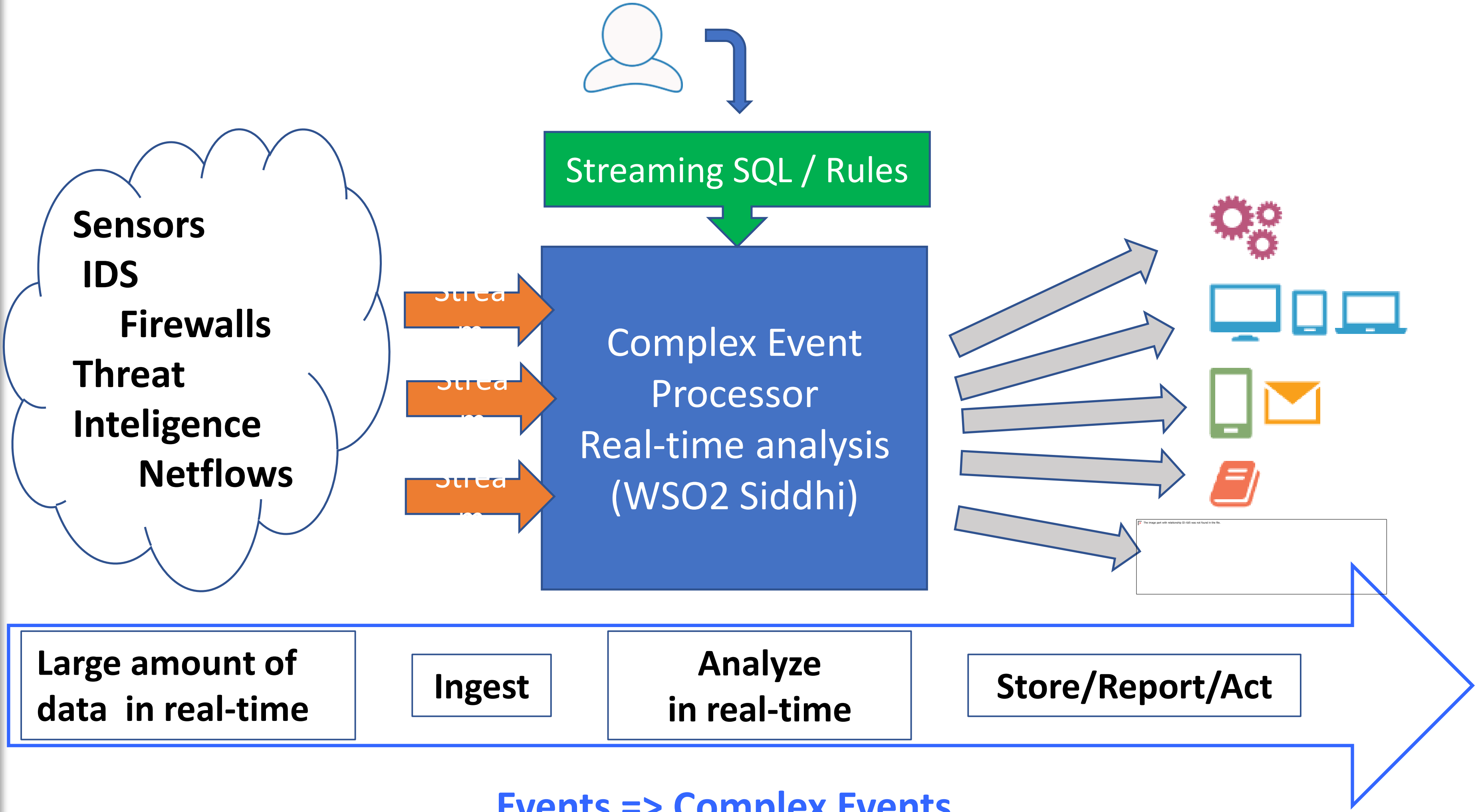
Hybrid systems

BigData paradigm

Big Data paradigm for Cybersecurity



Complex Event processing



Sensors
IDS
Firewalls
Threat Inteligence
Netflows

Strea m

Strea m

Strea m

Streaming SQL / Rules

Complex Event Processor
Real-time analysis
(WSO2 Siddhi)

The image part with relationship ID rId5 was not found in the file.

Large amount of data in real-time

Ingest

Analyze in real-time

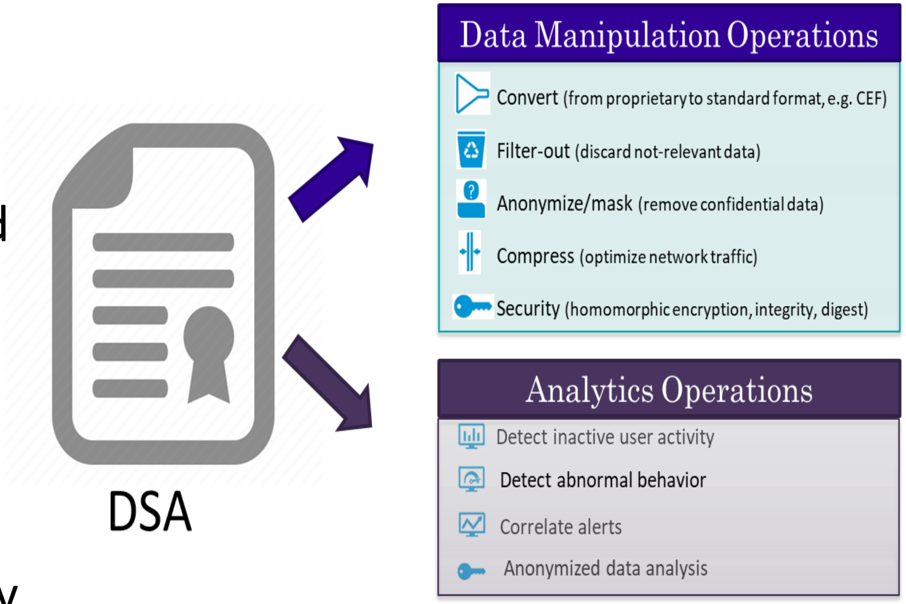
Store/Report/Act

Events => Complex Events

Data Sharing Agreements for CTI

C3ISP
Collaborative and Confidential Information
Sharing and Analysis for Cyber Protection

- **Data Sharing contracts for Data Analytics Services allowing confidential and trusted treatment of CTI:**
  - Empowering the data owners to protect their data from trusted and untrusted services , considering two extremes:
    - When the data analytics service is trusted we use just usage control mechanisms
    - When the data analytics is not trusted we can use homomorphic encryption (or anonymization) to allow collaborative and confidential analysis
  - Data usage control techniques, including sticky policies.



Data Manipulation Operations

- Convert (from proprietary to standard format, e.g. CEF)
- Filter-out (discard not-relevant data)
- Anonymize/mask (remove confidential data)
- Compress (optimize network traffic)
- Security (homomorphic encryption, integrity, digest)

Analytics Operations

- Detect inactive user activity
- Detect abnormal behavior
- Correlate alerts
- Anonymized data analysis

- **Enhancing security data analytics as a service:**
  - algorithms and services based data analytics for security

THANK YOU !

SHIELD – https://www.shield-h2020.eu/

PROTECTIVE – https://protective-h2020.eu/

C3ISP – https://c3isp.eu/

SHIELD

PROTECTIVE
PROACTIVE RISK MANAGEMENT

C3ISP
Collaborative and Confidential Information
Sharing and Analysis for Cyber Protection