Innoviris

Kick-off Secur'IT platform

BruFence

innoviris.brussels
empowering research

September 8, 2015

ULB

UCL Université catholique de Louvain

BruFence - goals

Design of mechanisms based on machine learning and big data mining techniques that allow sensible and secure systems to automatically detect attacks and fraudulent behaviours

BruFence - goals

Two main domains of application:

(i) automatic detection of threats and attacks against communication systems
(research sponsored by Steria Belux)

(ii) automatic detections of frauds in large amount of transactions
(research sponsored by Worldline and Nviso)

BruFence

- Constant evolution and unpredictability of attacker techniques
- Recent attacks/frauds highlight the ineffectiveness of security based on static rules inspired by known attacks
  (antivirus, firewalls, classical IDS, application proxies…)

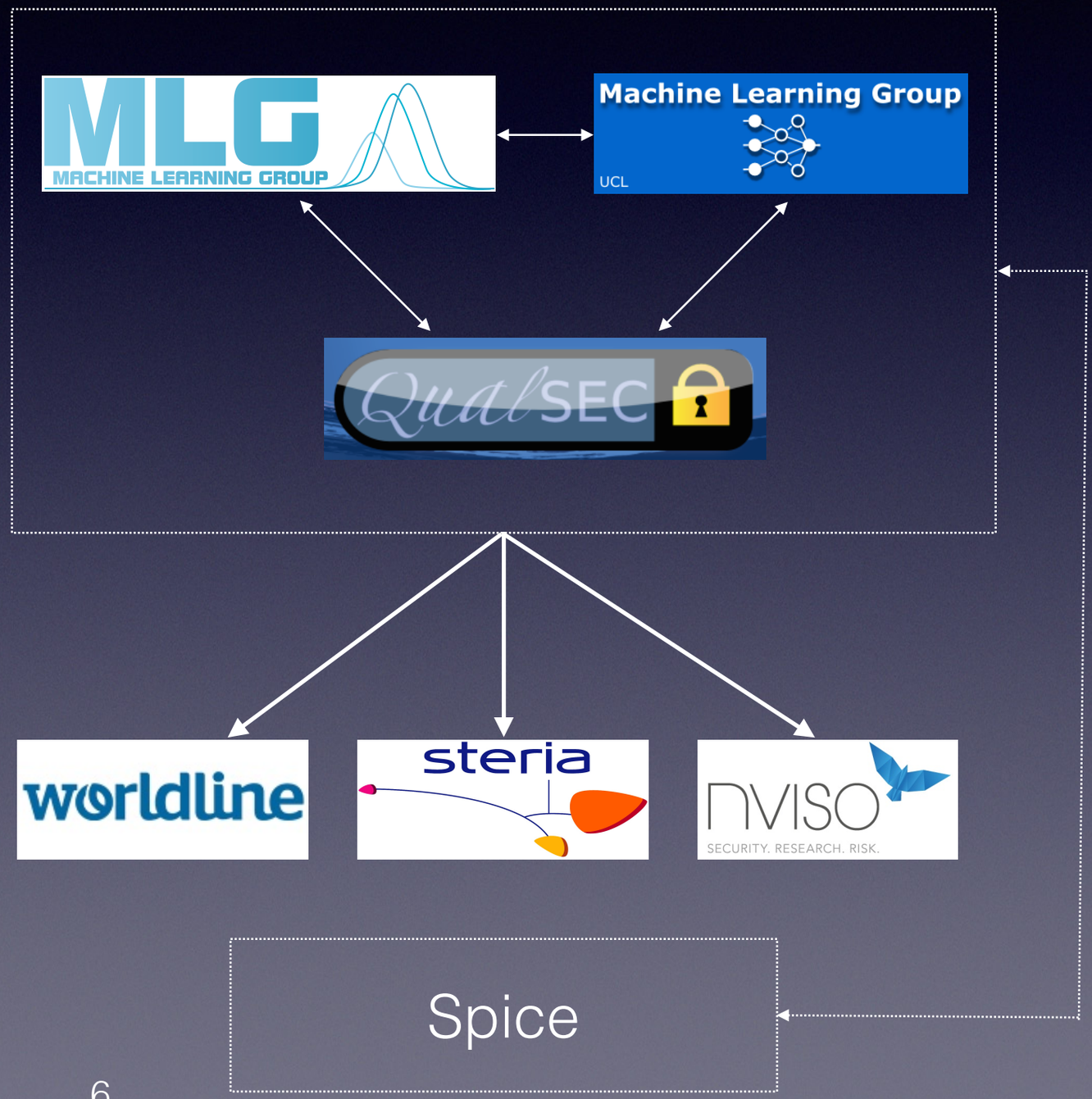
BruFence - goals

Enable automatic improvements of the defenses by:

- detecting abnormal behaviour in its data level processes
- tracing the actions done during an attack/fraud
- exploiting (social) network data

BruFence - consortium

- ULB - QualSec
- ULB - MLG
- UCL - MLG
- Wordline
- Steria
- NViso



Threats detection techniques

Design of mechanisms for automatic detection of threats and attacks in Managed File Transfer systems and Collaboration Platforms (Sharepoint, …)

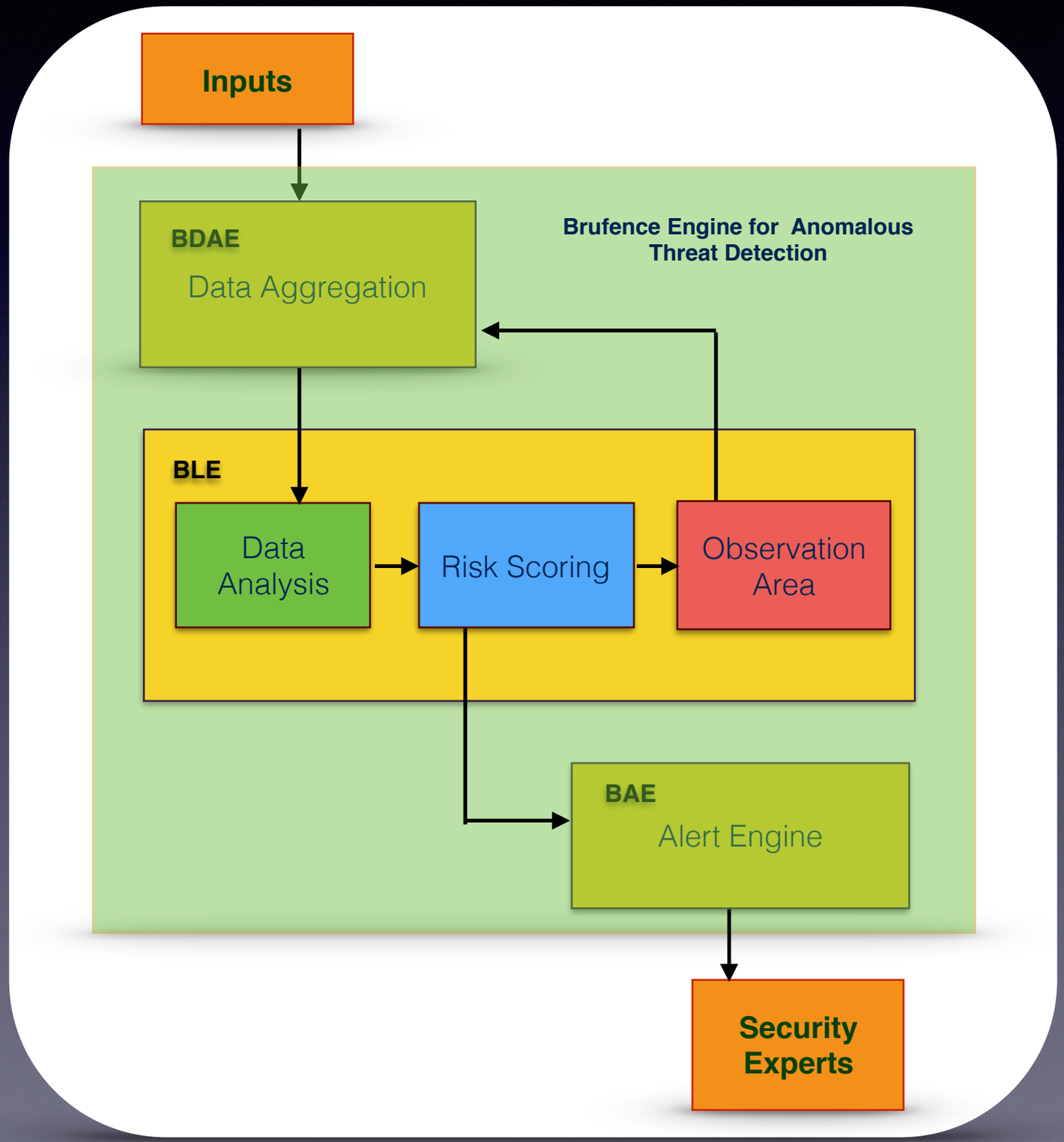
Machine Learning for threats detection based on *Outlier* Detection Analysis

Outliers: data points or sequences of multiple data points recognised as deviations from the remaining ‘normal’ data

Threats detection techniques

- Data-centric risk management modular approach (for the detection of Advanced Persistent Threats, Zero-day attacks, DDoS attacks, …)
- Spatial locations, temporal aspects, …
- Observation areas (using *honeypots* and *sandboxes)*

Threat and Attack detection in collaboration platforms and managed file Transfer



Scalable fraud detection techniques

Scalable fraud detection platform for transactional data based on machine learning techniques for Big Data

Million of transactions: large volume of data (Big Data)

Maximum 6 sec available to make predictions (fraud or genuine)

High unbalance between the classes (fraudulent transactions are 0.2%)

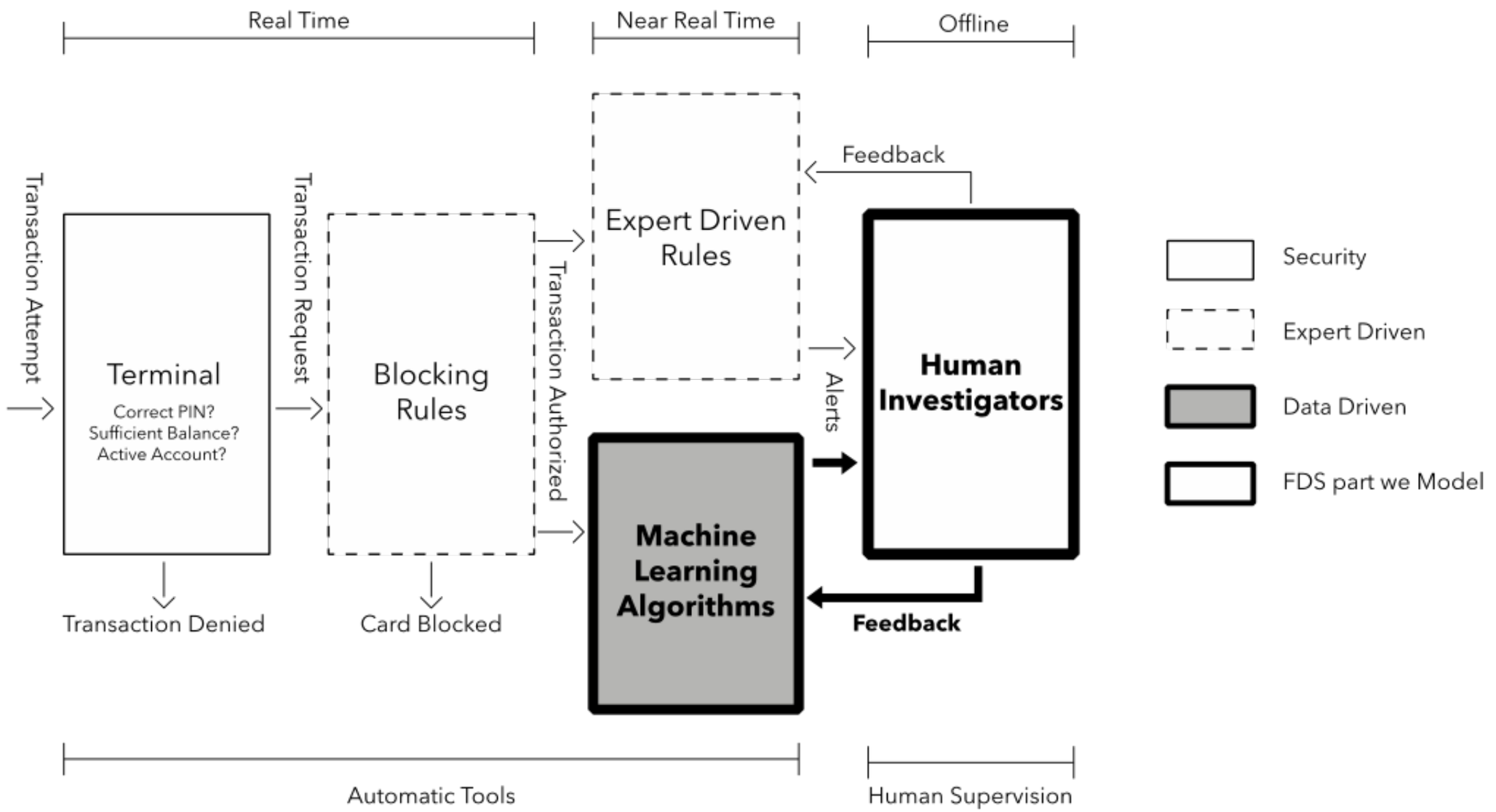
Scalable fraud detection techniques

Two main programs form the platform:

1. the **Stream manager** that collects and classifies the transactional data stream

2. the **Model developer** that updates the model for the classification

Fraud detection system design



Networks to enhance frauds and threats detection

- Improving the frauds and threats detection rate by using graph information

- For example: use of graph structures of relations between card holders, merchants and transactions

Networks to enhance frauds and threats detection

Sensitive information retrieval from social networks

- Classification of individuals in social networks
- Inferring private and/or sensitive information from the structure and the data of social networks

Networks to enhance frauds and threats detection

Network Criticality

- The aim is to detect the most *critical* or *vulnerable* nodes or actors in a graph or network

Scalability issues

- Terabytes of (sometimes linked) data are to be analyzed

BruFence

Thank you