Beyond Gut Instincts: Understanding, Rating and Comparing Self-Learning IDSs

International Conference On Cyber Situational Awareness, Data Analytics and Assessment.

June 8-9, 2015, London, UK

Settanni, Giuseppe

Digital Safety and Security Department

Austrian Institute of Technology

Vienna, Austria

Context

- **ECOSSIAN EU-FP7 Project**
- **E**uropean **Co**ntrol **S**ystem **S**ecurity **I**ncident **A**nalysis **N**etwork
- 19 European Partners;
- 3 years duration,
- 13 M€ budget.
- **GOAL:** Improve the **detection** and **management** of highly sophisticated cyber security **incidents** and **attacks** against **critical infrastructures** by implementing a pan-European **early warning** and **situational awareness** framework with command and control facilities.

Motivation

- **Problem:**
  - APTs result in financial loss and tarnished reputation
  - Long time until discovery (> 1 year)
  - Many companies affected
- **Countermeasures:**
  - Intrusion Detection Systems (IDS)
  - And other security solutions
- **Missing:**
  - Mechanisms to
    - Rate
    - Compare
    - Evaluate existing security solutions

Objectives

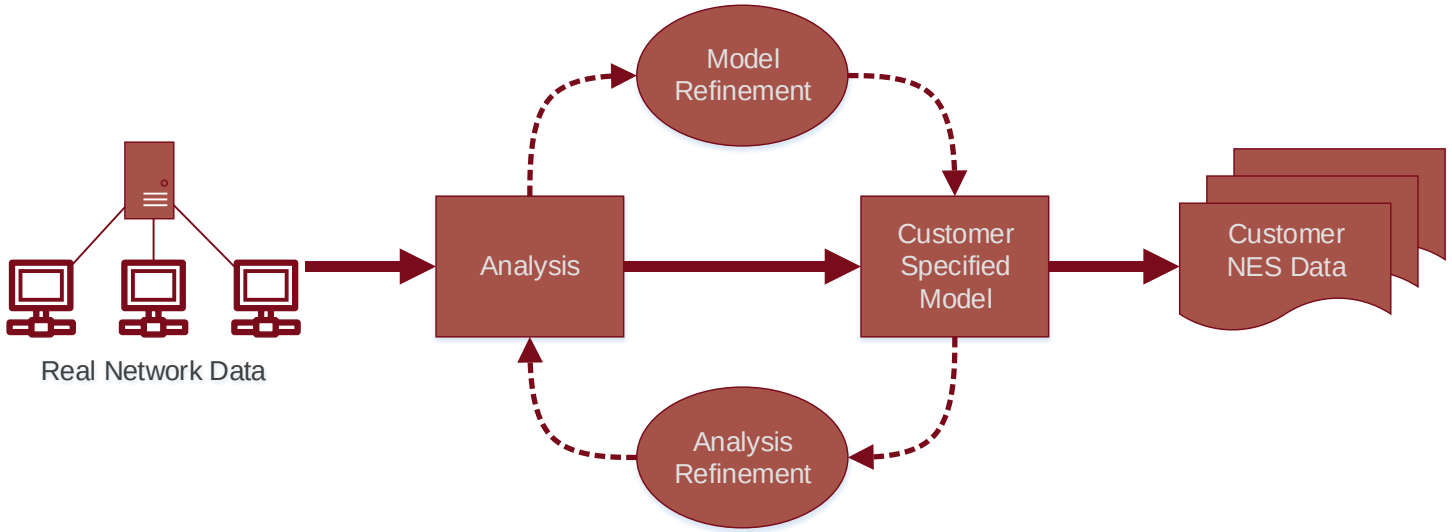
- Vendor independent
  - Rating
  - Comparing
  - Evaluating of IDSs
- Find security solutions for customer-specific infrastructures
- Speed up procurement, configuration and integration at low costs

BÆSE – **B**enchmarking and **A**nalytic **E**valuation of IDSs in **S**pecified **E**nvironments

Scientific Goals and Innovations (1/2)

Generating realistic **Network Event Sequence** (NES) data for customer-specified environments:

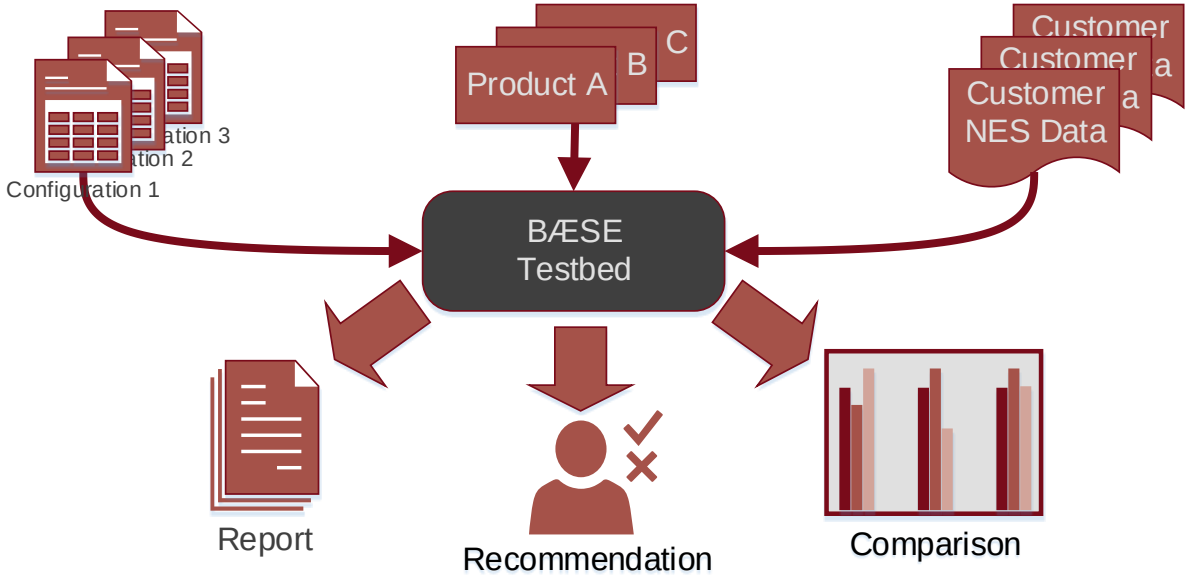
- Novel analytic approach
- Based on properties of a running, customer-defined infrastructure
- Customizable model complexity for scalable evaluation, ranging from quick to in-depth assessment



Scientific Goals and Innovations (2/2)

Evaluation of IDSs with customer NES data by using **BÆSE**:

- Rate, analyse and improve self-learning IDSs
- Compare different IDS solutions with respect to customer requirements
- Detect most effective configuration parameters
- Establish new metrics to compare different IDSs in terms of detection capabilities



Application Areas

- Cyber Security Solution Providers:
  - Rate new products in network infrastructures of various size and shape
  - Adapt existing products to specific customer requirements
  - Estimate market potential of future IDSs

- End-users
  - Find optimal security solution in shorter time
  - Find most efficient configuration
  - Rate and improve security mechanisms easily
  - Save money and time in operation and set up

Research Progress

- ✓ Design of a model for generating NES data based on log data
  - Methods: log line clustering, Markov chain simulation
- ✓ Consolidated expertise on IDSs:
  - AECID (*Automated Event Correlation for Incident Detection*)

- **Future work:**
  - Research on metrics for comparing different IDSs
  - Implementation of BÆSE testbed
  - Integration of prototype in ECOSSIAN system

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

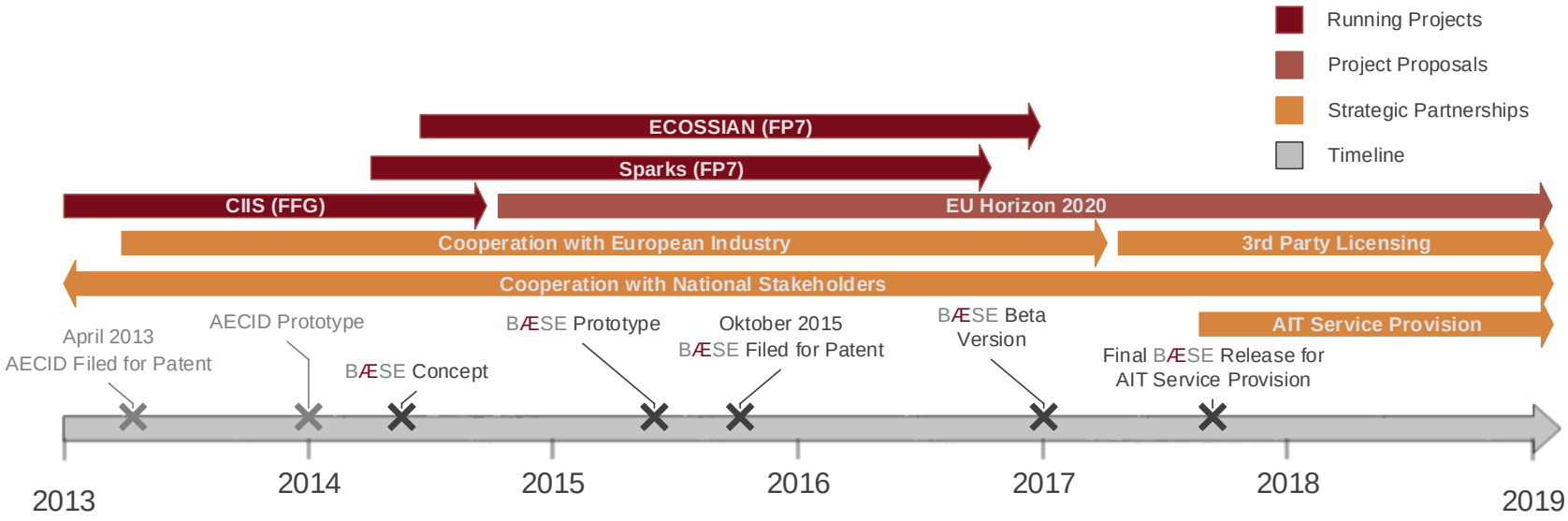
Thank you!

Giuseppe Settanni, MSc
Junior Scientist, ICT Security
Business Unit Information Management
Digital Safety and Security Department

giuseppe.settanni@ait.ac.at | +43 664 88390671 | www.ait.ac.at/it-security

Backup slides

Timeline


Running Projects
Project Proposals
Strategic Partnerships
Timeline
ECOSSIAN (FP7)
Sparks (FP7)
CIIS (FFG)
EU Horizon 2020
Cooperation with European Industry
3rd Party Licensing
Cooperation with National Stakeholders
AIT Service Provision
April 2013
AECID Filed for Patent
AECID Prototype
BÆSE Concept
BÆSE Prototype
Oktober 2015
BÆSE Filed for Patent
BÆSE Beta Version
Final BÆSE Release for AIT Service Provision
2013
2014
2015
2016
2017
2018
2019

Market Situation

- **Rising costs** caused by cyber attacks
- Solution providers do not know the **specific requirements** of their customer‘s infrastructures (→ Customer NES Data)
- **Select a suitable security solution** for a customer infrstructure to detect sophisticated and tailored cyber attacks like APTs
- There is no vendor independent market-ready solution to **compare IDSs in terms of applicability** for customer specific environments
- It is **not cost-efficient** for customers to **find the best configuration** for their infrastructure

Business Cases

- AIT provides BÆSE as service
  - Consulting of partner companies
- AIT sells licences to IT services and consulting companies
- Concrete business case:
  - Company places an order
  - Afterwards delivers a set of real network data
  - Consulting company generates NES Data and uses BÆSE to find the most accurate security solution for the customer
  - Consulting company delivers the optimal security solution for the specific customer infrastructure