Wi-fi: MARRIOT_CONFERENCE
EVDT04

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Break-out 2 – Foundational technical methods and risk management for trustworthy systems

Chair: Chair: Brian Lee, Athlone IT & PROTECTIVE

cyberwatching.eu
The European watch on cybersecurity & privacy

Participants

Break-out 2 – Foundational technical methods and risk management for trustworthy systems

Family Name	First Name	Project
Bernabe	Jorge Bernal	ANASTACIA
Aubigny	Matthieu	ATENA
Martinelli	Fabio	C3ISP
Rios	Davis	CYBECO
Bessani	Alysson	DiSIEM
Crespo	Alberto	FENTEC
Votis	Konstantinos	GHOST
Khoffi	Ismail	HERMENEUT
Slamanig	Daniel	PRISMACLOUD
Lee	Brian	PROTECTIVE
Koeune	Francois	REASSURE
Zwingelberg	Harald	SPECIAL
Puccetti	Armand	VESSEDIA

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Dr. Jorge Bernal Bernabe

University of Murcia

https://webs.um.es/jorgebernal

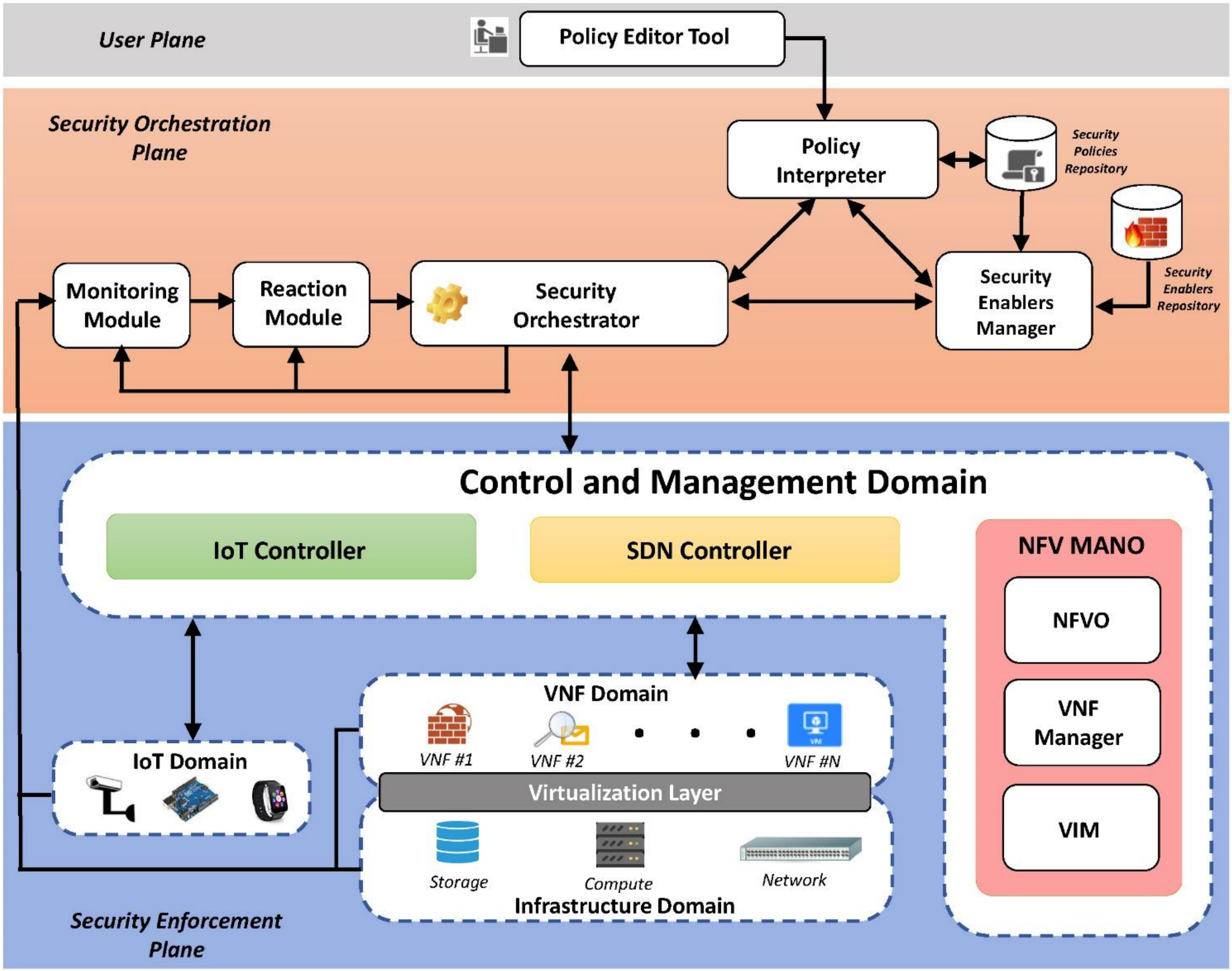
ANASTACIA

http://anastacia-h2020.eu

ANASTACIA Project Objectives, challenges & results for end users

- ANASTACIA is developing a trustworthy-by-design security framework able to take autonomous decisions with networking technologies such as **SDN**, **NFV** and **intelligent and dynamic security enforcement** and monitoring methodologies and tools.
- The ANASTACIA **cyber-security framework** will provide **self-protection**, self-healing and self-repair capabilities through novel enablers and components in **CPS and IoT**.
- Dynamically **orchestrate** and deploy user **security policies** and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures
- **Monitoring and reaction** and techniques will allow more automated adaptation to mitigate new and unexpected security vulnerabilities
- Scenarios for influential business sectors: **MEC , BMS**
- **Achievements** so far (1st Year)
  - Project on track. Deliverables, architecture, requirements and scenarios defined, papers and events…
  - First version of Policy-based system implemented, First demos available
  - Monitoring, reaction components and SIEM tools being adapted to IoT scenarios with SDN/NFV
  - network security functions deployed as VNFs → defense mechanisms and threat countermeasures, including vFirewall, vIDS/IPS, vAAA, vChannelProtection, vIoTHoneyNet…
- **Result for end users**:
  - Self-protection→ dynamic mitigation and countering cyber-attacks
  - Intuitive user-friendly tools to model and configure policies governing the security in CPS/IoT.

ANASTACIA



User Plane

Policy Editor Tool

Security Orchestration Plane

Policy Interpreter

Security Policies Repository

Security Enablers Repository

Monitoring Module

Reaction Module

Security Orchestrator

Security Enablers Manager

Control and Management Domain

IoT Controller

SDN Controller

NFV MANO

NFVO

VNF Manager

VIM

VNF Domain

VNF #1

VNF #2

VNF #N

Virtualization Layer

IoT Domain

Storage

Compute

Network

Infrastructure Domain

Security Enforcement Plane

ANASTACIA Project next steps & collaboration opportunities

- Next steps in Anastacia
  - First **demonstrator**
    - implement different use cases related to the MEC and BMS
    - validate the proposed architecture
    - Evolve the cyber-security framework with the feedback obtained
- Collaboration opportunities
  - Look into new virtual network security functions (**vNSF**) for IoT/CPS
  - **Security/privacy** protocols in **IoT**: AAA, Network Access, KeyManagement, ChannelProtection
  - **Monitoring** agents, SIEM for IoT/CPS scenarios
  - Deal with new kind of evolving **attacks** in IoT/CPS
    - e.g. Low-rate attacks in IoT, Zero-days attacks
  - Explore **marching learning** techniques for the reaction components

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

ATENA

Matthieu AUBIGNY

itrust consulting

itrust
consulting

ATENA Project Objectives

Improve Security and Resilience capabilities of ICT-based Critical Infrastructures against a wide variety of cyber-physical threats (malicious attacks or unexpected faults) which may affect Essential Services

Domains of main interest are service utilities:

- electrical generation/distribution
- water treatment/distribution
- gas distribution
- Smart Grid

LEONARDO
SECURITY & INFORMATION SYSTEMS
itrust consulting
חברת החשמל
Israel Electric
SAPIENZA
creos
Multitel
La société wallonne des eaux
UNIVERSIDADE DE COIMBRA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
FCTUC
ENEA
Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile
uni.lu
UNIVERSITÉ DU LUXEMBOURG
CRAT
ROMA TRE
UNIVERSITÀ DEGLI STUDI
Institute of Baltic Studies

ATENA Project challenges and results

- ✓ Models to control physical flow efficiency and improve resilience across CIs against threats of their IACSs and related ICT infrastructures
- ✓ Distributed Intrusion and Anomaly Detection System (IADS) using Big Data technology to early detect anomalous behavior state including smart probes
- ✓ New anomaly detection algorithms and risk assessment methodologies within a distributed Cyber-Physical environment
- ✓ Methodologies and technologies for increasing auto-reconfiguring capability of ICT-controled CIs for resilience of Cyber-Physical systems
- ✓ A suite of integrated ICT networked components for detection and reaction in presence of adverse events in industrial distributed systems
- ✓ Validation of the ATENA models and tool suite in significant business-oriented Use Cases

ATENA Project next steps & collaboration opportunities

Finalize Integration of developed subsystem

Partnership with stakeholders for industrial integration

Industrials sectors

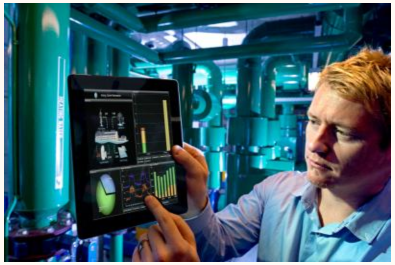
Validation on near-real environnement

Collaboration to improve security standardisation for Smart-Grid, IoT, Privacy

Standards

Demonstrate the concept to end-users

Collaboration with hardware and software manufacturers on smart detection, mitigation, risk assessment systems



cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Fabio Martinelli, CNR

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

cyberwatching.eu
The European watch on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

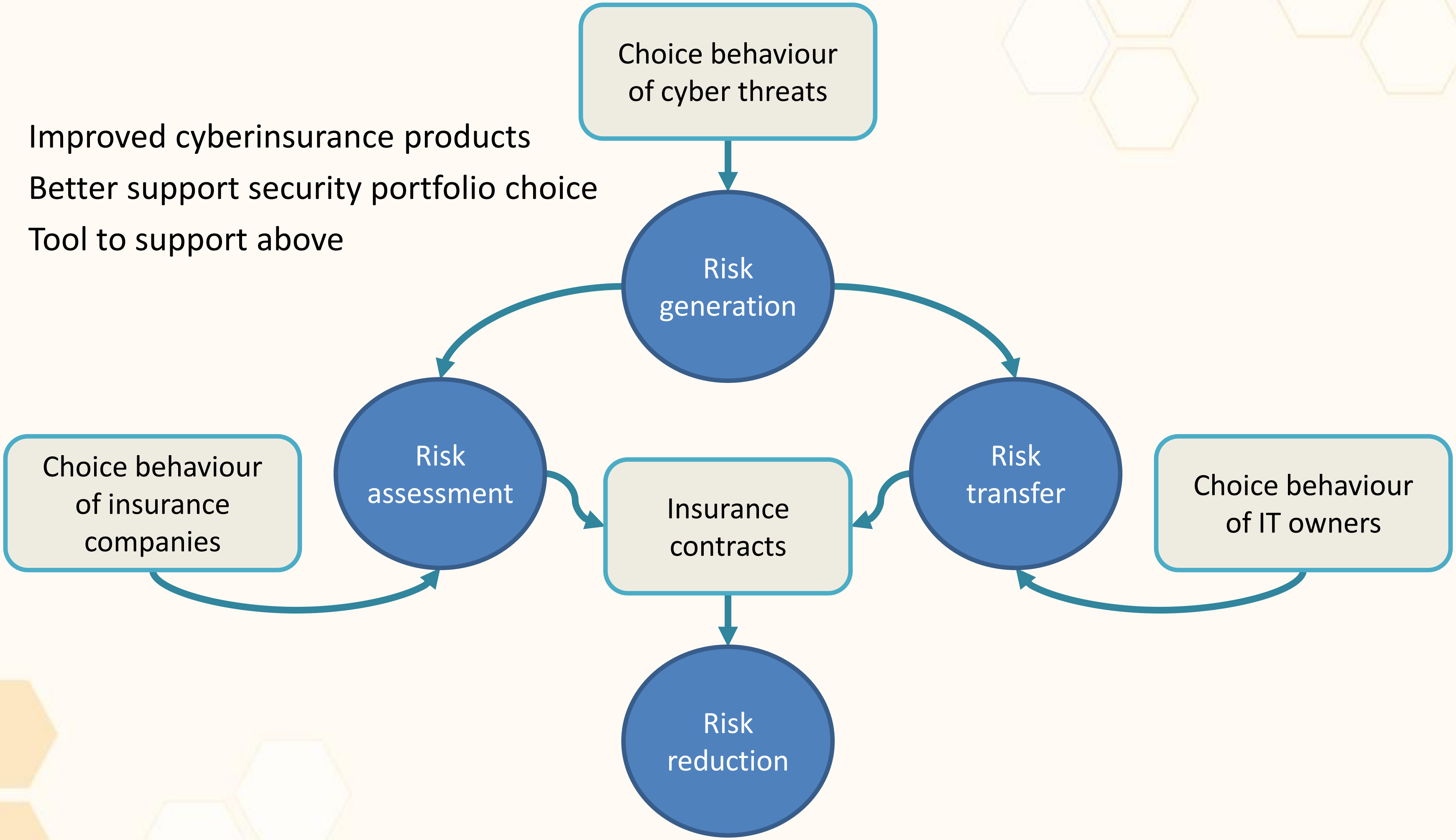
Brussels, Belgium

David Ríos Insua

CYBECO

Objectives, challenges & results for end users

- Improved cyberinsurance products
- Better support security portfolio choice
- Tool to support above


Choice behaviour of cyber threats
Risk generation
Risk assessment
Risk transfer
Choice behaviour of insurance companies
Insurance contracts
Choice behaviour of IT owners
Risk reduction

Next steps & collaboration opportunities

- Perform experiments
- Complete CYBECO tool and case studies
- Refine methodology and tool
- Complete policy analysis to feed exploitation plan

Collaborations welcome!!

- Try our methodology and help test tool
- Take part in experiments
- Share datasets
- Impact models
- Cyberinsurance ecosystem
- Join our final conference

https://www.cybeco.eu

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

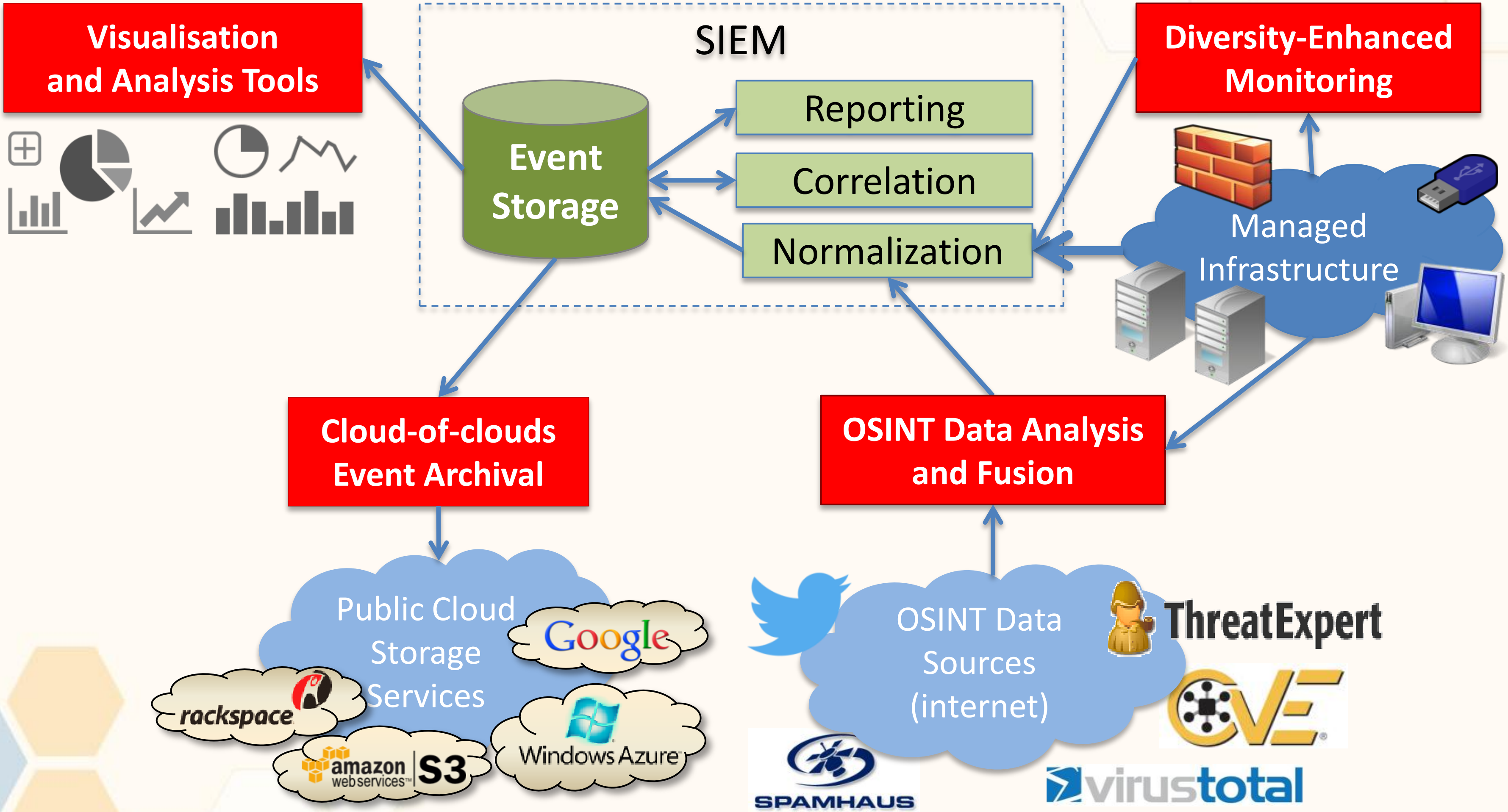
Brussels, Belgium

Alysson Bessani

DISIEM

Objectives, challenges & results

- **Objective:** improve existing SIEMs



Visualisation and Analysis Tools
SIEM
Event Storage
Reporting
Correlation
Normalization
Diversity-Enhanced Monitoring
Managed Infrastructure
Cloud-of-clouds Event Archival
OSINT Data Analysis and Fusion
Public Cloud Storage Services
Google
rackspace
amazon webservices S3
Windows Azure
OSINT Data Sources (internet)
ThreatExpert
CVE
SPAMHAUS
virustotal

Next steps & collaboration opportunities

- Technology, research, validation…
  - **SIEMs**: Arcsight, Splunk, XL-SIEM, ElasticSearch
  - **Topics**: OSINT processing, visual analysis, machine learning for security, prediction, cloud integration
  - **Validation**: Amadeus, EDP, and ATOS environments
- Collaboration opportunities:
  - Joint dissemination activities
  - Users of our technologies
  - Exploitation opportunities

http://disiem-project.eu

DiSIEM

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

ALBERTO CRESPO, Atos Spain S.A.

FENTEC

FENTEC Project Objectives, challenges & results for end users

- Objectives - Functional ENcryption TEChnologies
  - Enable fine-grained access to encrypted data, programs executed on such data => novel FE crypto, HW concepts
- Challenges: develop new application-oriented FE
  - General-purpose, versatile and efficiently computable FE
  - Adequate security-efficiency-expresiveness trade-off
- Results for end-users
  - **Unified API of FE functions** suitable to decrypt arbitrary functions enabling enhanced security of complex systems (compartmentalization)
  - **3 real-life scenarios**: digital currency, anonymous data analytics, secure Local Decision Making (LDM) for IoT

FENTEC Project next steps & collaboration opportunities

- Materialize progress (Conceptual, Practical, Implementation) levels:
  - 09/18: Requirements, prototype func. analyses, security/trust models
  - 04/19: 1st Spec. of FE Schemes
  - 08/19: 1st impl. of FE Schemes
  - 12/19: First piloting cycle starts

- Close collaboration with other Cybersecurity PPP Actions (esp. in Cryptography -DS-06-2017- PROMETHEUS, PRIViLEDGE, FutureTPM) and exchange experience on:
  - Technical foundations to enhance security of complex systems and for balancing functionality/security/efficiency
  - Approaches to improve performance incl. novel HW concepts (tamper-resistant cryptographic HW)
  - Increased trustworthiness (less need for explicit trust)

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

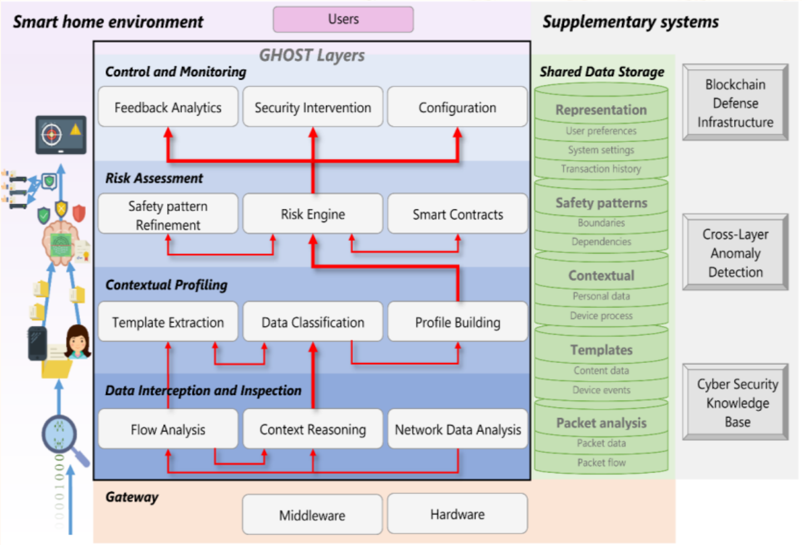
26 April 2018
Brussels, Belgium

Konstantinos Votis

GHOST

GHOST Project Objectives, challenges & results for end users

- Objectives
  - Usable and effective security framework for smart home residents
  - User-centric cyber security architecture for smart home environments
  - Safeguard critical security-related data using blockchain technology



- Challenges and results for end users
  - GHOST will equip end users with their own cyber security inspection, discovery and decision toolset
  - Usable security solution to address users’ tendency to choose convenience over security

GHOST Project next steps & collaboration opportunities

- A first version of the core security components has been designed and implemented
- Integration is ongoing
- First prototype is expected for the first trial runs (June 2018)

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

Ahmed Bounfour
Professor, Paris-Sud University,
Scientific Coordinator, HERMENEUT
Ahmed.bounfour@u-psud.fr

cyberwatching.eu

The European watch on cybersecurity & privacy

HERMENEUT Objectives

HERMENEUT Goals

1/ Improve the **assessment of organizations' vulnerabilities**

asset identification
tangible and **intangible** assets at risk
the business plans of the attacker
the commoditisation level of the target organisations
the exposure of the target
the human factors

HERMENEUT Goals

2/ improve the **estimation of the consequences of cyber-attacks**

innovative micro- and macroeconomic cost model
focus on intangible costs

HERMENEUT Goals

3/ Integrate all the above with a **holistic risk assessment model**

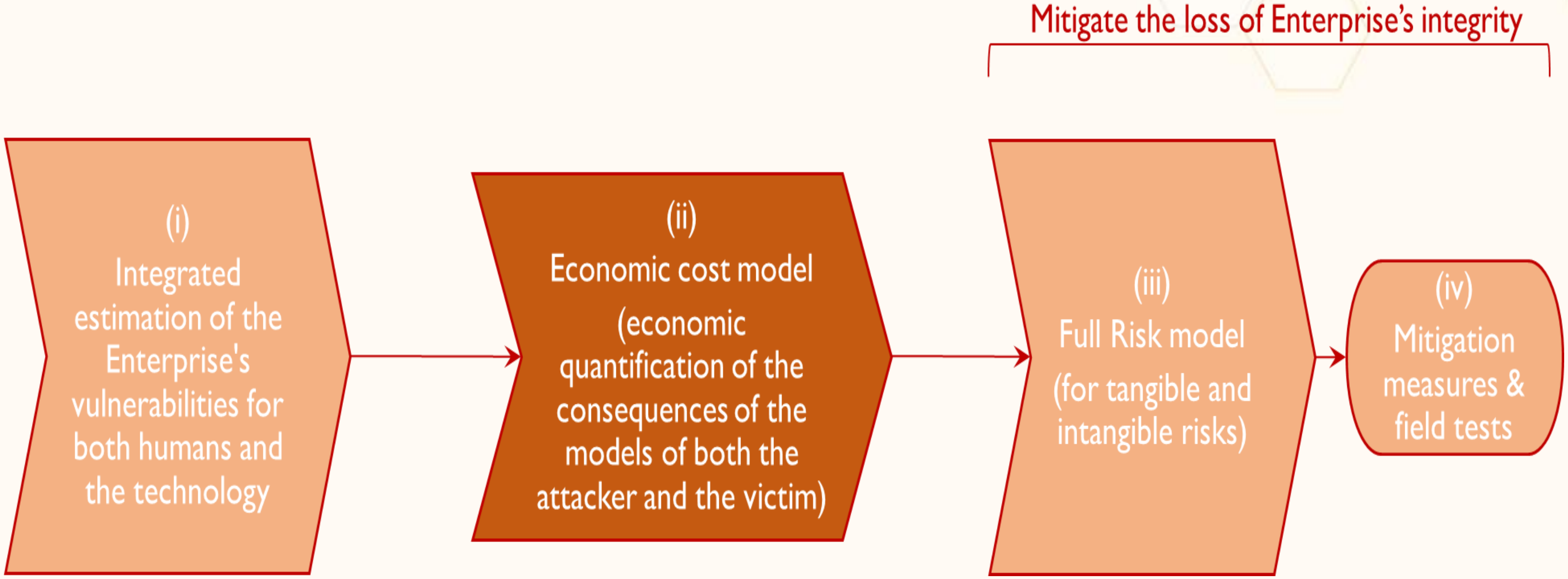
to support cyber-security investment decisions

hard (traditional) and soft **mitigation measures** integrating: dedicated elicitation approaches and

Benefit-Harm Index (BHI)

Supporting both **individual organisation** level and **industrial sector** level

HERMENEUT Approach


Mitigate the loss of Enterprise's integrity
(i)
Integrated estimation of the Enterprise's vulnerabilities for both humans and the technology
(ii)
Economic cost model
(economic quantification of the consequences of the models of both the attacker and the victim)
(iii)
Full Risk model
(for tangible and intangible risks)
(iv)
Mitigation measures & field tests

create a holistic approach to cyber-security cost-benefit analysis

HERMENEUT Validation

4 key market sectors:

- Healthcare
- IP-intensive Industries
- Financial services
- Retail

A **White Paper** for each sector
using publicly available data sources
complemented by elicited expert knowledge
provide strategic guidance on the necessary
investments to reduce cyber-risks
focusing on soft mitigation measures.

Project next steps & collaboration opportunities

- Economics of the impact of cyberattacks, especially with regards to the intangible dimension , both at Micro and Macro levels
- Providing the best estimates of the impact and its related risk
- Proposals of guidelines on the likelihoods of the attacks as well as on countermeasures taking into account sectoral specificities

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018
Brussels, Belgium

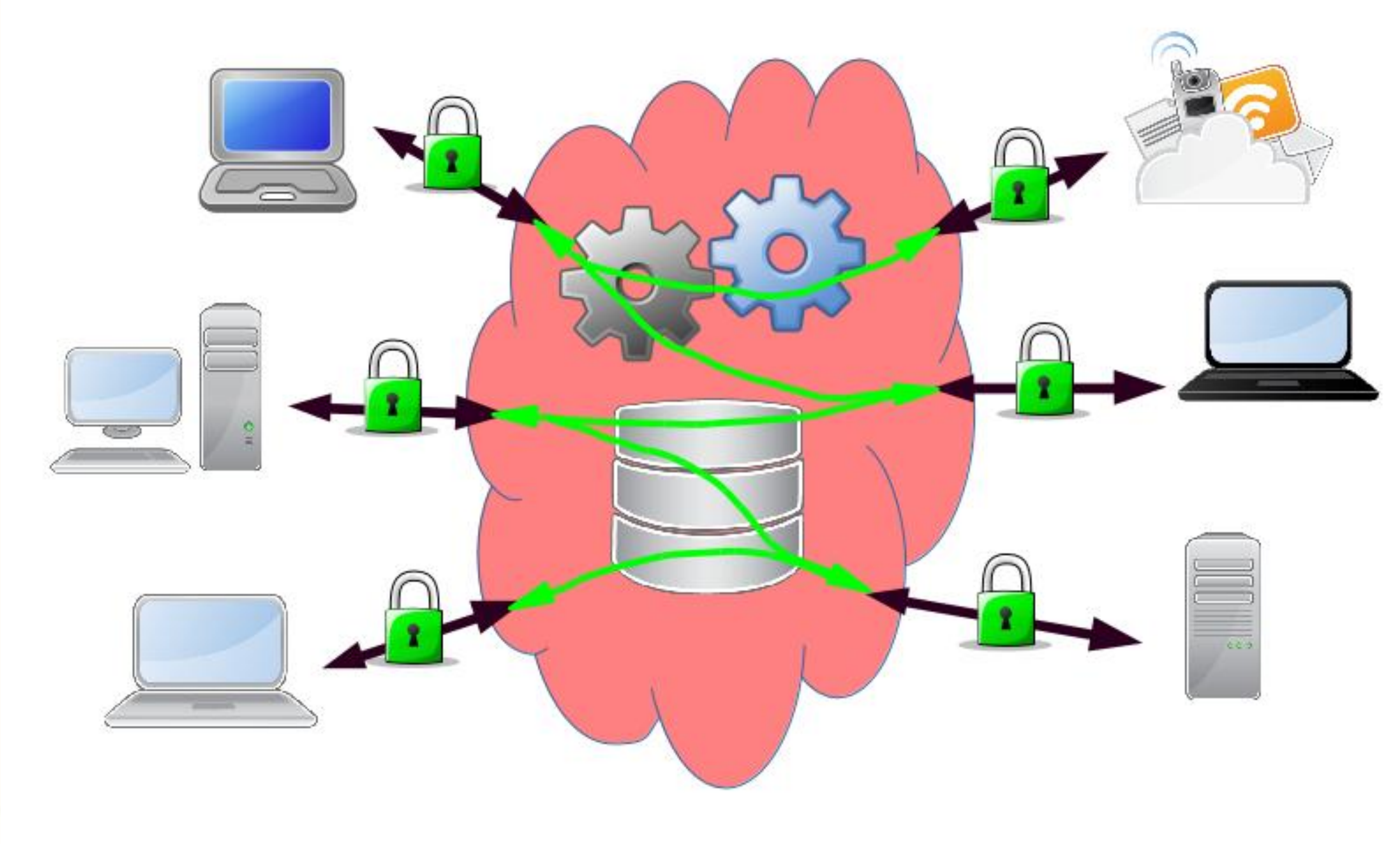
Dr. Daniel Slamanig

prisma cloud

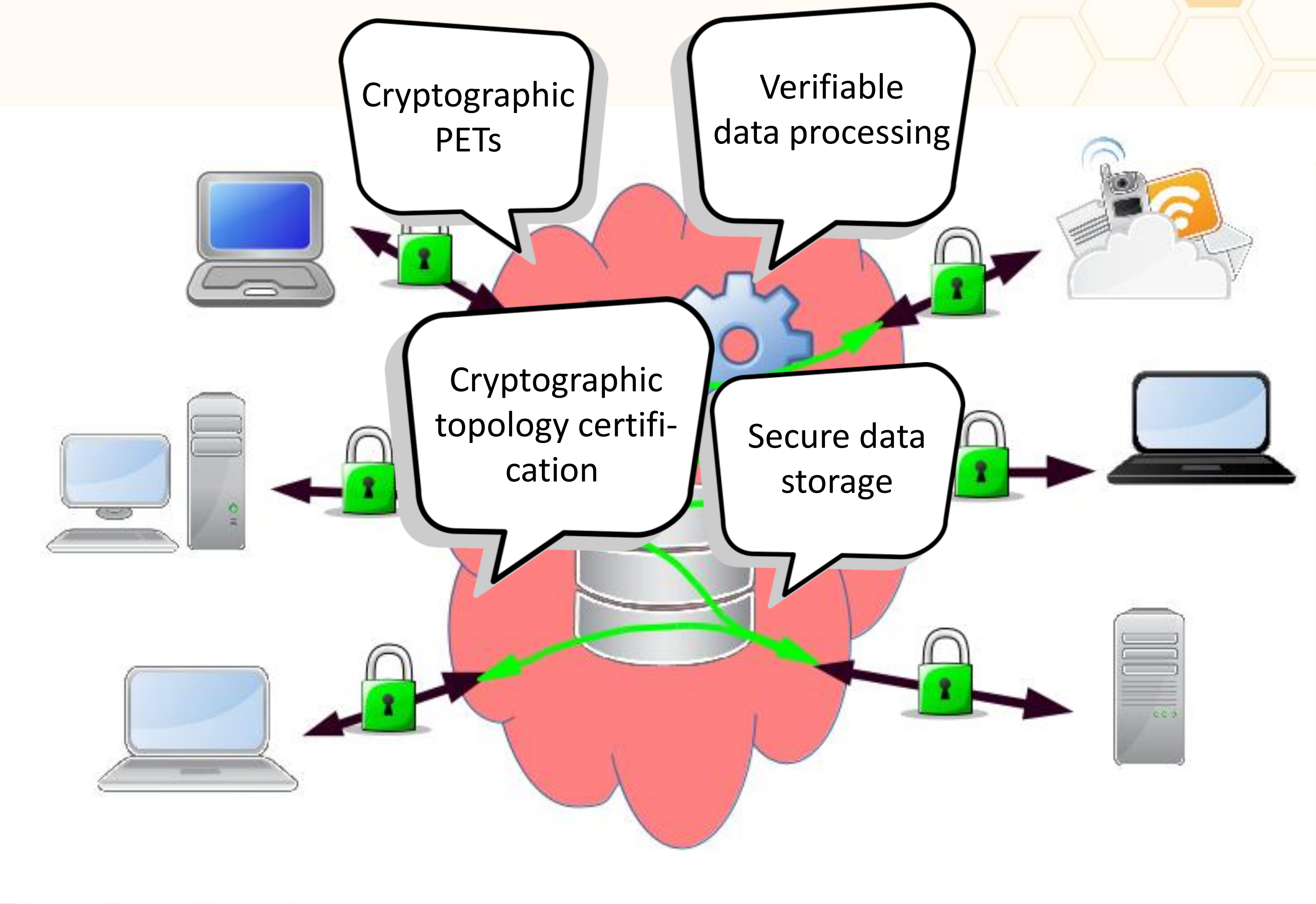
PRIvacy and Security MAintaining services in the CLOUD

PRISMACLOUD - Vision

The **main idea and ambition** of PRISMACLOUD is to **enable end-to-end security** for cloud users and provide tools to **protect their privacy** with the best technical means possible - **by cryptography.**



PRISMACLOUD - Vision



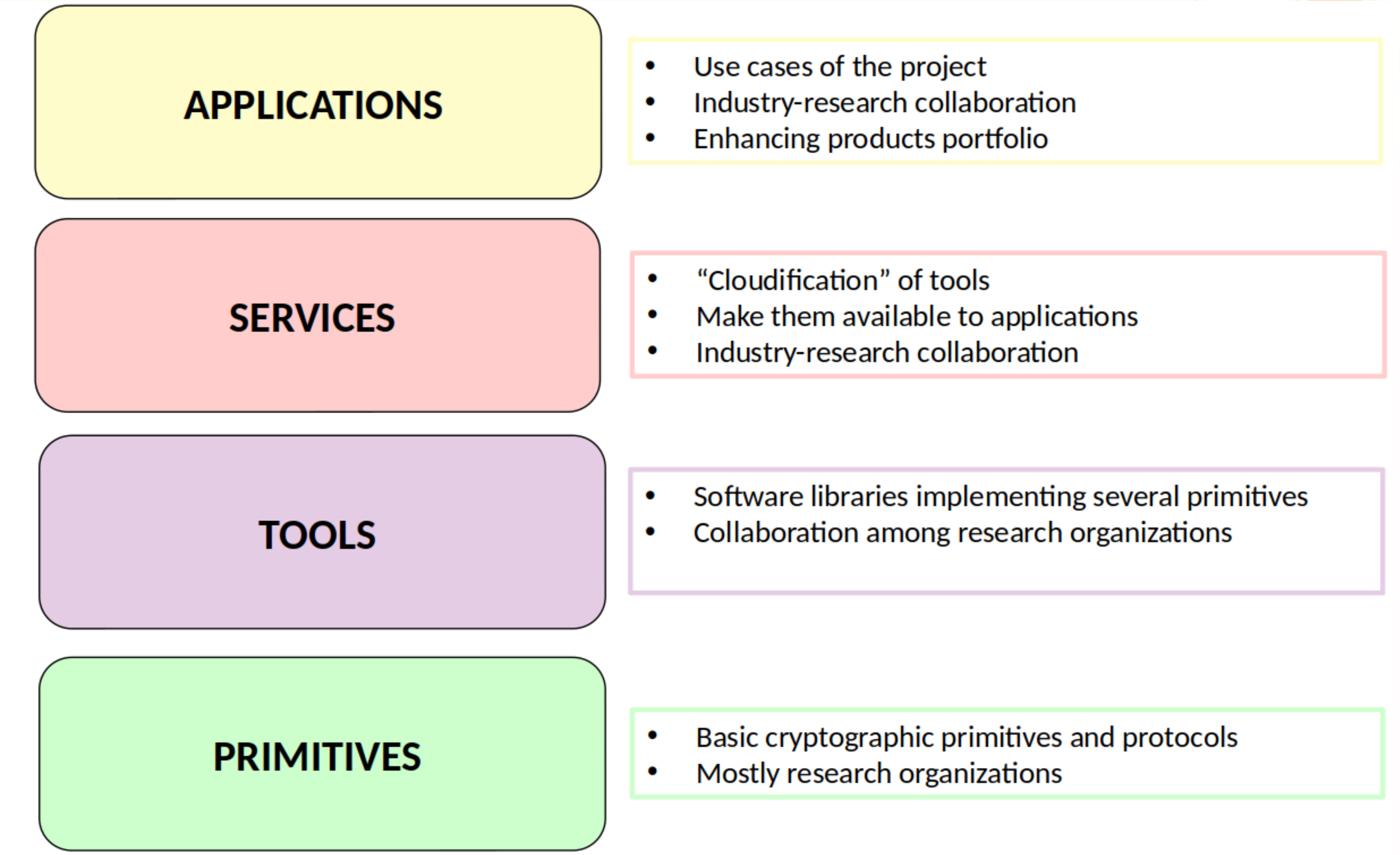
Cryptographic PETs

Verifiable data processing

Cryptographic topology certification

Secure data storage

PRISMACLOUD Project Objectives, challenges & results



APPLICATIONS

- Use cases of the project
- Industry-research collaboration
- Enhancing products portfolio

SERVICES

- "Cloudification" of tools
- Make them available to applications
- Industry-research collaboration

TOOLS

- Software libraries implementing several primitives
- Collaboration among research organizations

PRIMITIVES

- Basic cryptographic primitives and protocols
- Mostly research organizations

PRISMACLOUD Project next steps & collaboration opportunities

- Advanced cryptography implemented in tools and services
- Piloting of developed tools and services within use-cases ongoing
- Standardization of advanced cryptography

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

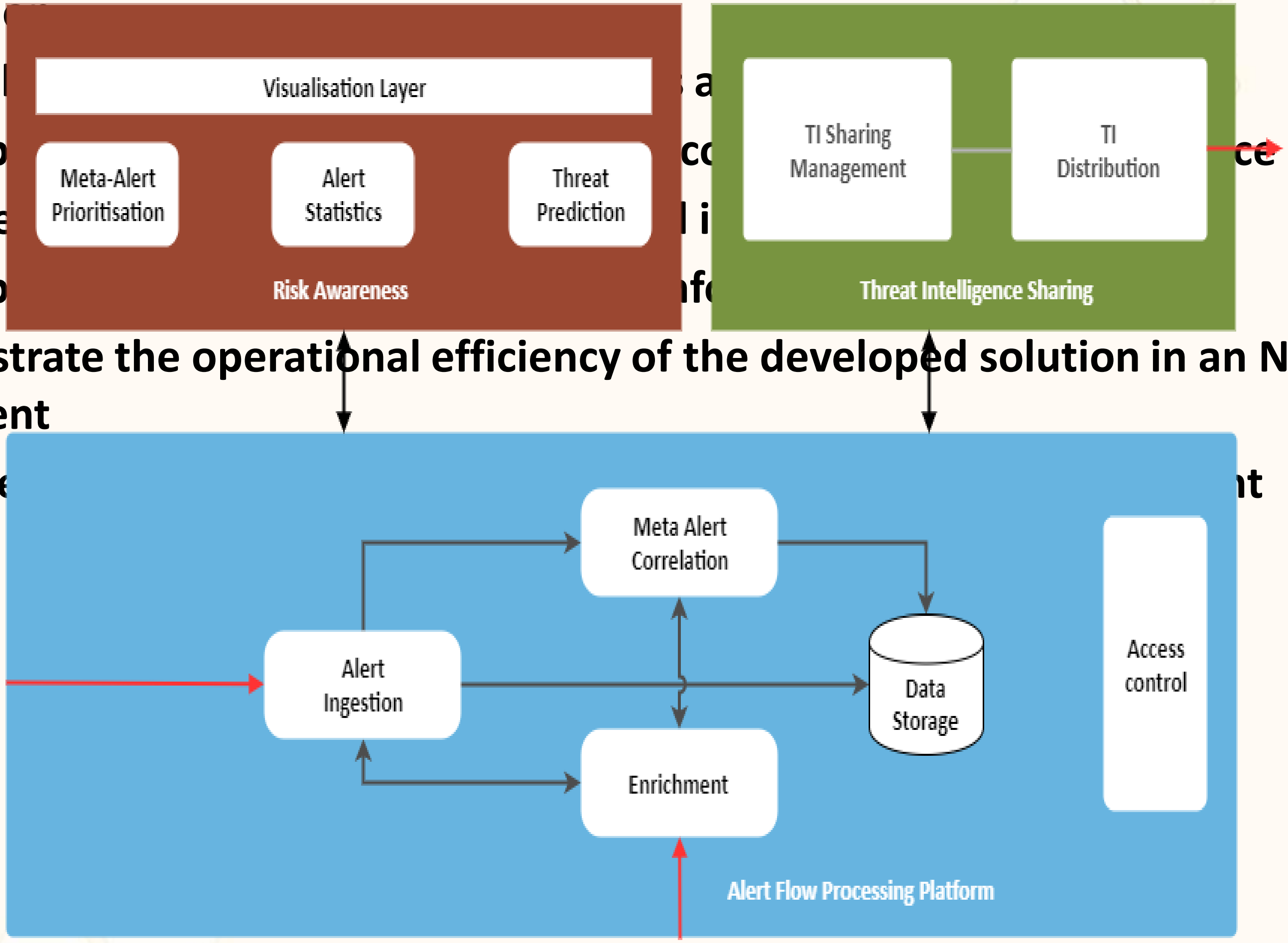
BRIAN LEE

PROTECTIVE

PROACTIVE RISK MANAGEMENT

PROTECTIVE Project Objectives, challenges & results for end users

- To enhance security oni ng t ugh improved incident correlation and prioritisati
- To establis a
- To develop co ce sharing
- To improve l i
- To develop nf
- To demonstrate the operational efficiency of the developed solution in an NREN environment
- To evaluate nt



PROTECTIVE Project next steps & collaboration opportunities

- Pilot 1 –NREN (Pol., Czech., Rom.) Feb-July
- Pilot 2 – Software Delivery
  - July
  - Sept
- Pilot 2 – NREN/SME
  - Jan – July 2019
  - Possibility to participate through TI sharing either giving or receiving !

cyberwatching.eu

The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

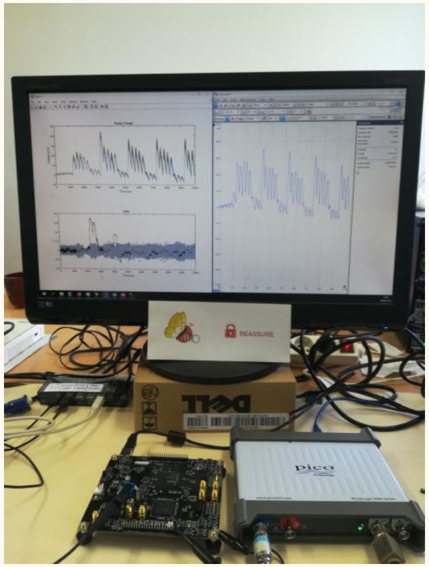
Brussels, Belgium

François KOEUNE

REASSURE

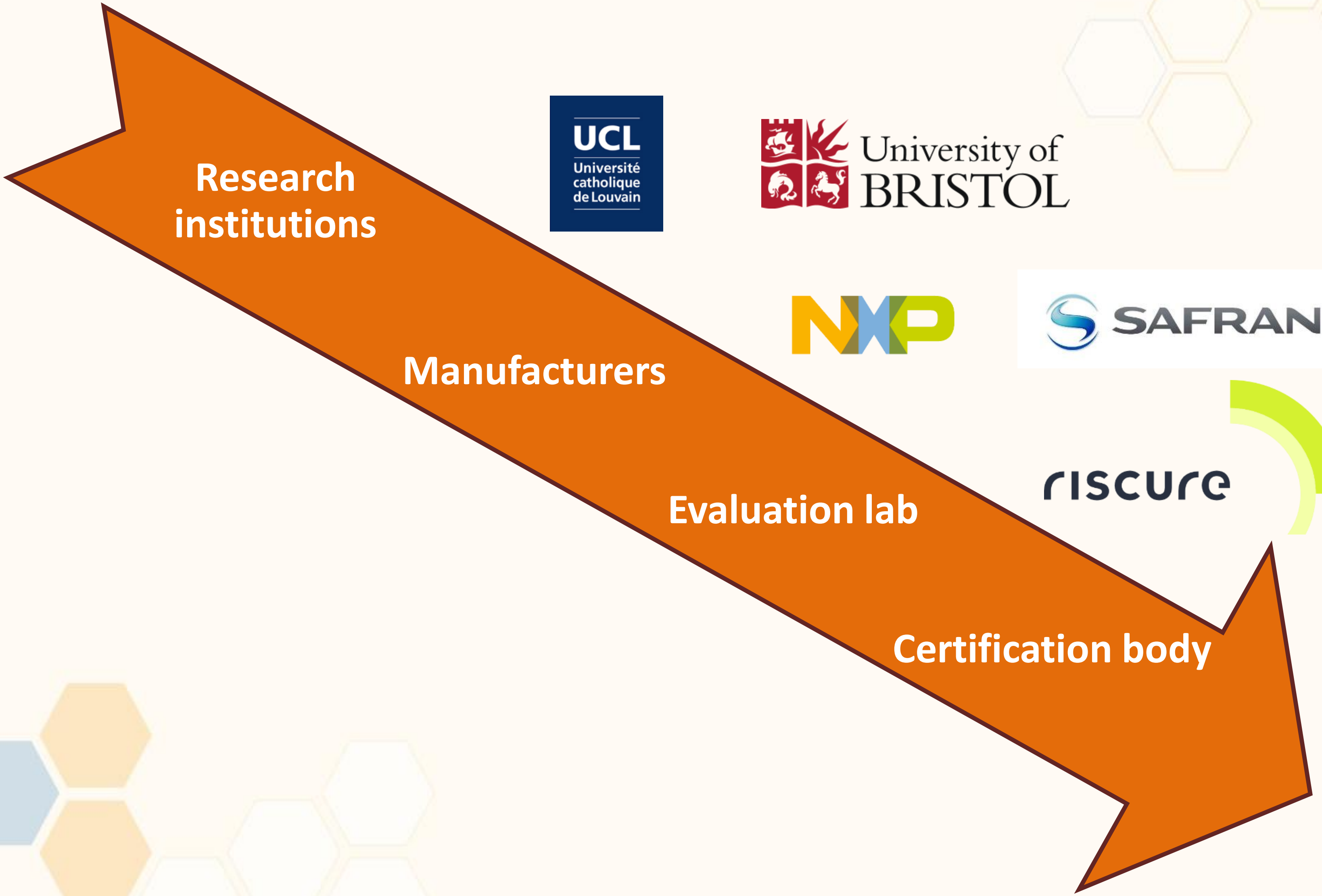
REASSURE objectives

- Improve embedded devices security against side-channel attacks (power, EM,…)
  - Best practices, semi-automated tools, reference data for evaluators
    - For the specialist (designers, evaluation labs)
    - For the newcomer (IoT, …)



➢ Sounder, more efficient, comparable assessment

REASSURE consortium: actors from the whole chain



Research institutions

Manufacturers

Evaluation lab

Certification body

UCL Université catholique de Louvain

University of BRISTOL

NXP

SAFRAN

riscure

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

REASSURE next steps & collaboration opportunities

- Autumn 2018: tutorial & walk-and-explore session
- Tutorial: leakage detection
  - Which test methodologies, which parameters?
  - How to interpret results (false negative/positive)?
- Walk-and-explore, “hands-on” session
  - Test methods, practice with tools…
- For more info: francois.koeune@uclouvain.be

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

SPECIAL

Harald Zwingelberg

SPECIAL Project

Scalable Policy-awareLinked Data Architecture
For Privacy, Transparency and Compliance

SPECIAL's Project Objectives, challenges & results for end users

- SPECIAL platform for big data supporting:
  - Acquisition of user consent at collection time
  - Privacy-aware, secure workflows, transparency usage control and compliance verification
  - Robustness in terms of performance, scalability
  - Dashboard with feedback and control features making processing comprehensible and manageable for data subjects, controllers and processors
- Target groups for SPECIAL Results
  - Direct users of SPECIAL results will be data controllers for handling of personal data, managing consent, etc.
  - Data subjects will (re-)gain transparency and control over personal data

SPECIAL’s next steps & collaboration opportunities

- Iterations for implementation of the pilots
- Extend policy engine
- Incorporate ePrivacy Regulation once public
- W3C community group defining vocabulary:
  - Taxonomy of regulatory privacy Terms,
  - Taxonomy of personal data,
  - Taxonomy of purposes, etc.

⇒ Visit the workshop website at : https://www.w3.org/2018/vocabws/

- Collaboration welcome in community group, future workshops, etc.

⇒ Contact SPECIAL: https://www.specialprivacy.eu/about/contact

cyberwatching.eu
The European watch
on cybersecurity & privacy

First Cyberwatching.eu Concertation Meeting

26 April 2018

Brussels, Belgium

Dr. Armand Puccetti

Vessedia

Verification Engineering of Safety and Security Critical Industrial Applications

VESSEDIA Project Objectives, challenges & results for end users at M16

- **VESSEDIA** aims at enhancing the safety and security medium-criticality S/W, especially IoT. More precisely, making formal methods more accessible for application domains that want to improve the security and reliability of their software applications.
- **Results**:
  - 1) security requirements for IoT
  - 2) on-going use-cases analyses (Contiki, 6LowPAN, etc.) using C/C++/Java analysis tools
  - 3) Improved tools for the analysis of C/C++/Java: Frama-C and VeriFast
  - 4) combined modelling & specification tools for vulnerabilities detection at source code level
  - 5) (on-going) draft of ISO standard for V&V tools
  - etc.

VESSEDIA Project next steps & collaboration opportunities

- **Methodology** definition for IoT V&V.
- **Improved tools**: modular reasoning at system level, cooperating static (Frama-C) & dynamic analyses (AFL), parallelisation of proofs, new proof tactics and simplifier, new GUI, etc.
- **Complete analyses** of use-cases.
- Contributions to **Common Criteria** certification process, evaluation of tools using Cyber Grand Challenge code samples.
- Metrics, security evaluations and quality tests of tools.
- Collaboration with project CHARIOT for common workshops.

5 R&I Challenges

1.				
2.				
3.				
4.				
5.				

Top 5 Cross-cutting themes

1.				
2.				
3.				
4.				
5.				

Top 5 New collaboration opportunities and new ideas.

1.				
2.				
3.				
4.				
5.				