



SECURING AGAINST INTRUDERS AND OTHER THREATS  
THROUGH A NFV-ENABLED ENVIRONMENT

[H2020 - Grant Agreement No. 700199]

# Cybersecurity and Big Data, a necessary binomial

Exploring the collaboration between cybersecurity and Big Data through an awarded project.



ubiwhere



POLITECNICO  
DI TORINO



Telefonica



Agenzia per l'Italia Digitale  
Presidenza del Consiglio dei Ministri



# Cybersecurity agenda

---

The EU is determined to safeguard an online environment providing the highest possible freedom and security, for the benefit of everyone.

## The EU Objectives

- Increasing cybersecurity capabilities and cooperation
- Making the EU a strong player in cybersecurity
- Making the EU a strong player in cybersecurity

## The EU strategy

- Increasing cyber resilience;
- drastically reducing cybercrime;
- developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- developing the industrial and technological resources for cybersecurity;
- establishing a coherent international cyberspace policy for the EU and promote core EU values

# Cybersecurity, a funded area

---

As part of the EU cybersecurity strategy, the European Commission and the European Cyber Security Organisation (ECSO) [signed a cPPP on 5 July 2016](#).

- The EU will invest up to €450 million in this partnership, under its research and innovation programme [Horizon 2020](#). Cybersecurity market players are expected to invest three times more.
- The Digital Security calls in 2016 under H2020-DS-2016-2017 have been transformed into Cybersecurity PPP calls in 2017.
- Three calls for August 24th 2017: DS-06, DS-07, and DS-08.
- Despite there are not specific calls regarding Big Data and Cybersecurity, there are a lot of common aspects, specially in the Telco area.



# SHIELD

---

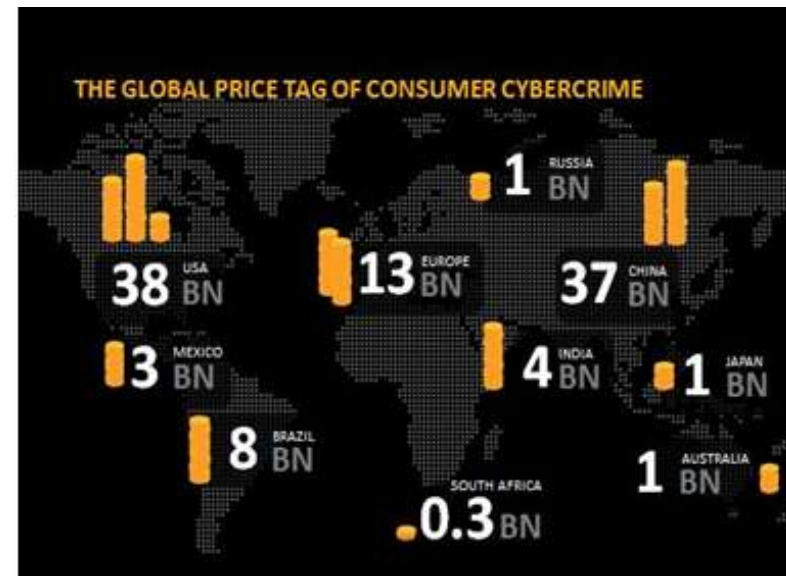
SHIELD- Securing against intruders and other threats through a NFV-enabled environment

- SHIELD was awarded with a 15/15 score.
- It was awarded under the DS-04-2015: Information driven Cyber Security Management
- Project coordinator is Space Hellas
- Technical coordinator is I2CAT.
- SHIELD is an example of the collaboration of the Telco, the Big Data and the Cybersecurity sectors.

# Motivation

## Problems

- Mobility & heterogeneity of devices.
- Volume, velocity and variety of data.
- Digitalization and globalization of the society.
- No effective collection of data.
- No reporting and sharing of data.
- Expensive and specialised hardware-based security appliances.



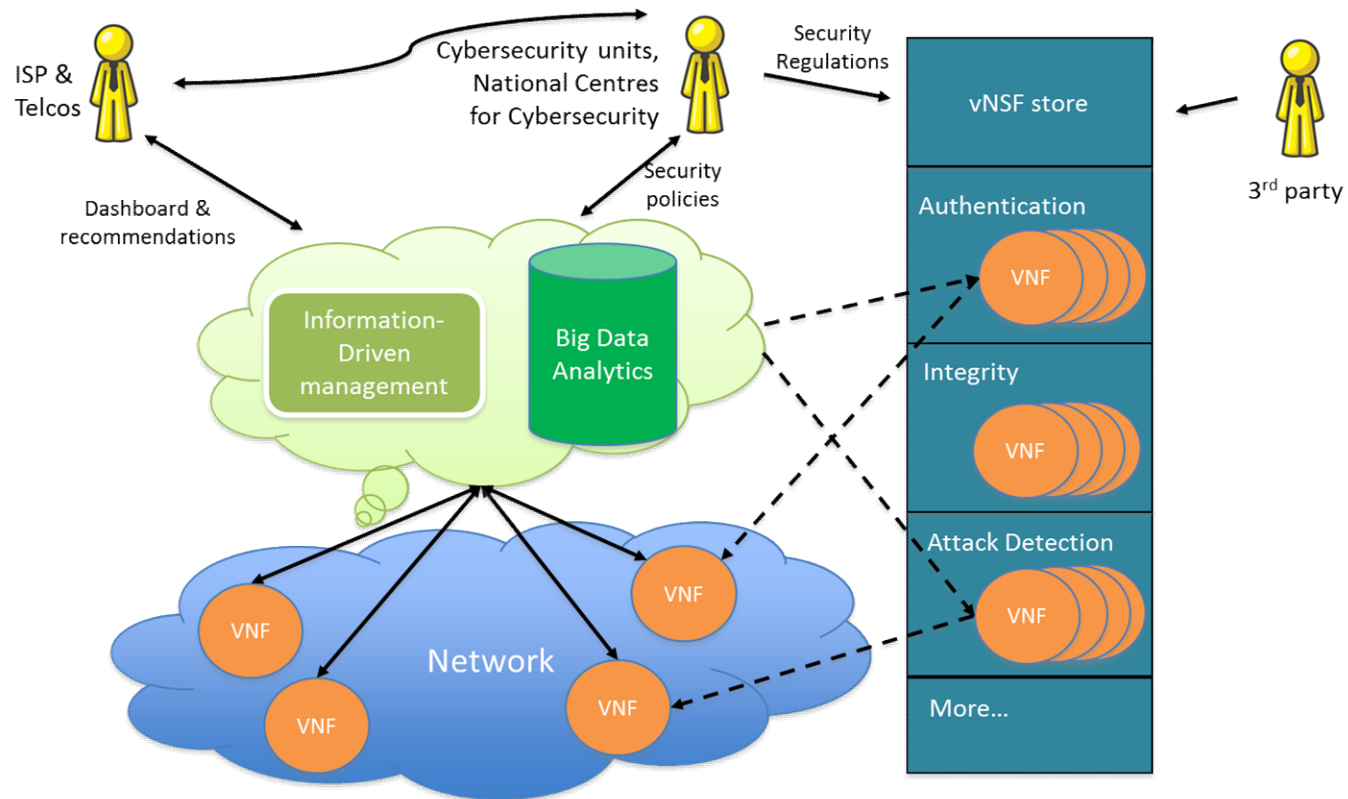
# Goal

---

- Create an IDP platform that
  - retrieves information from vNSFs deployed at strategic locations of the network
  - transmits such information to be properly processed by Big Data engines
  - visualises such information and recommend actions by means of a dashboard and accessible API
  - acts on the network for supplementary information acquisition or for taking effective counter-measures
  - provides flexible support for both new security capabilities and reconfiguration of existing security
  - is built on top of securized (attested) hardware



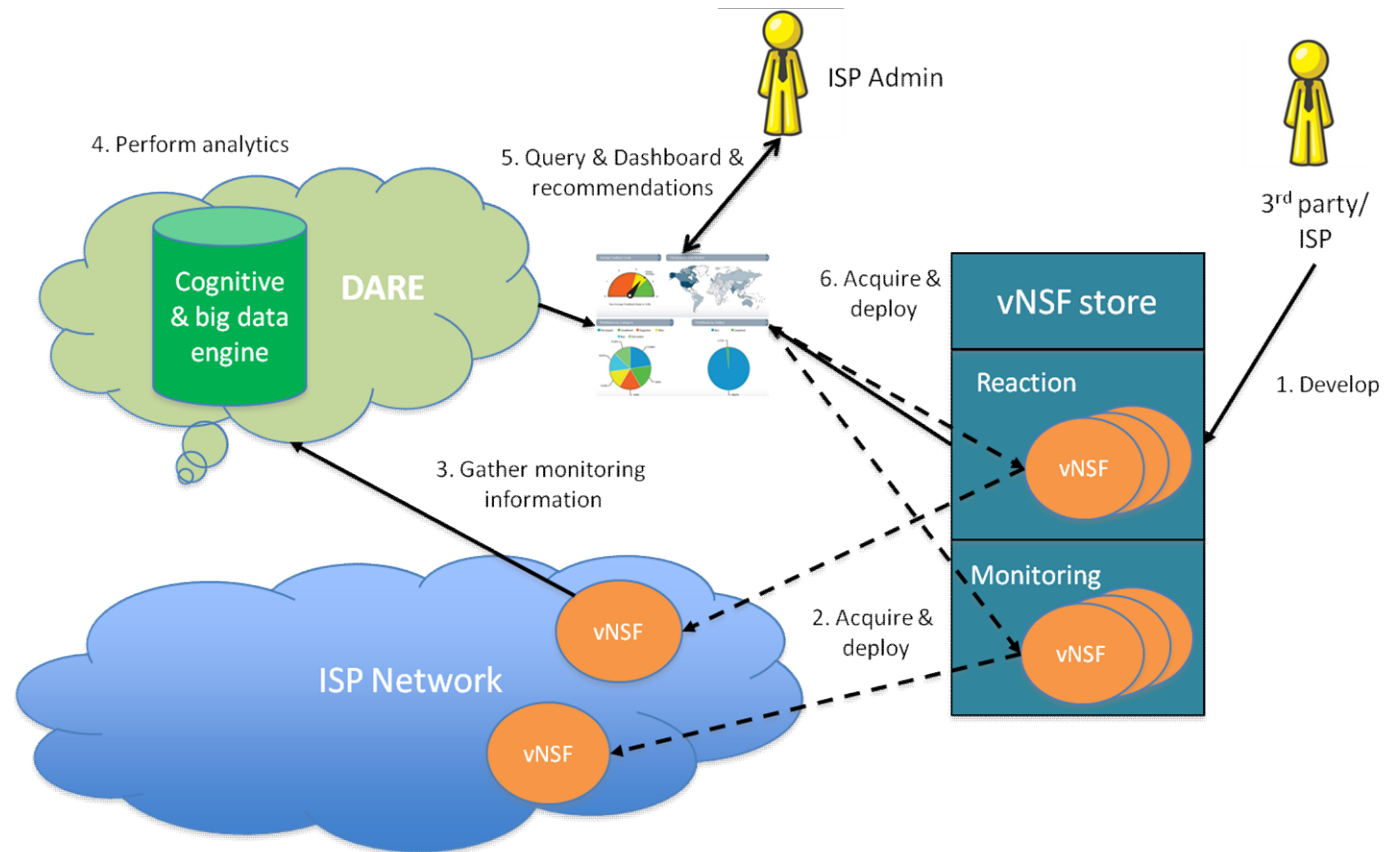
# Functional architecture



11

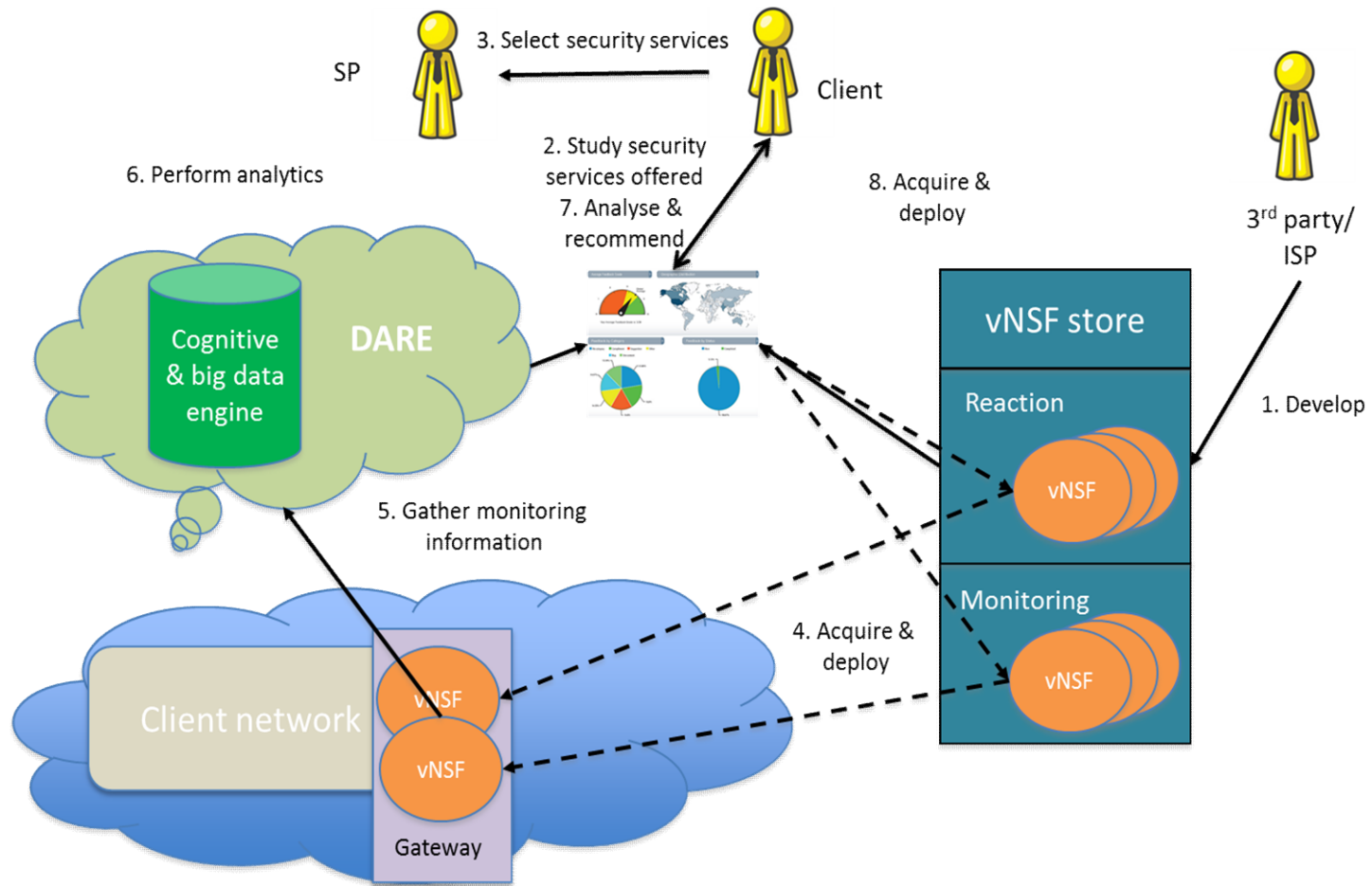


# Use-case 1: An ISP securing its own infrastructure

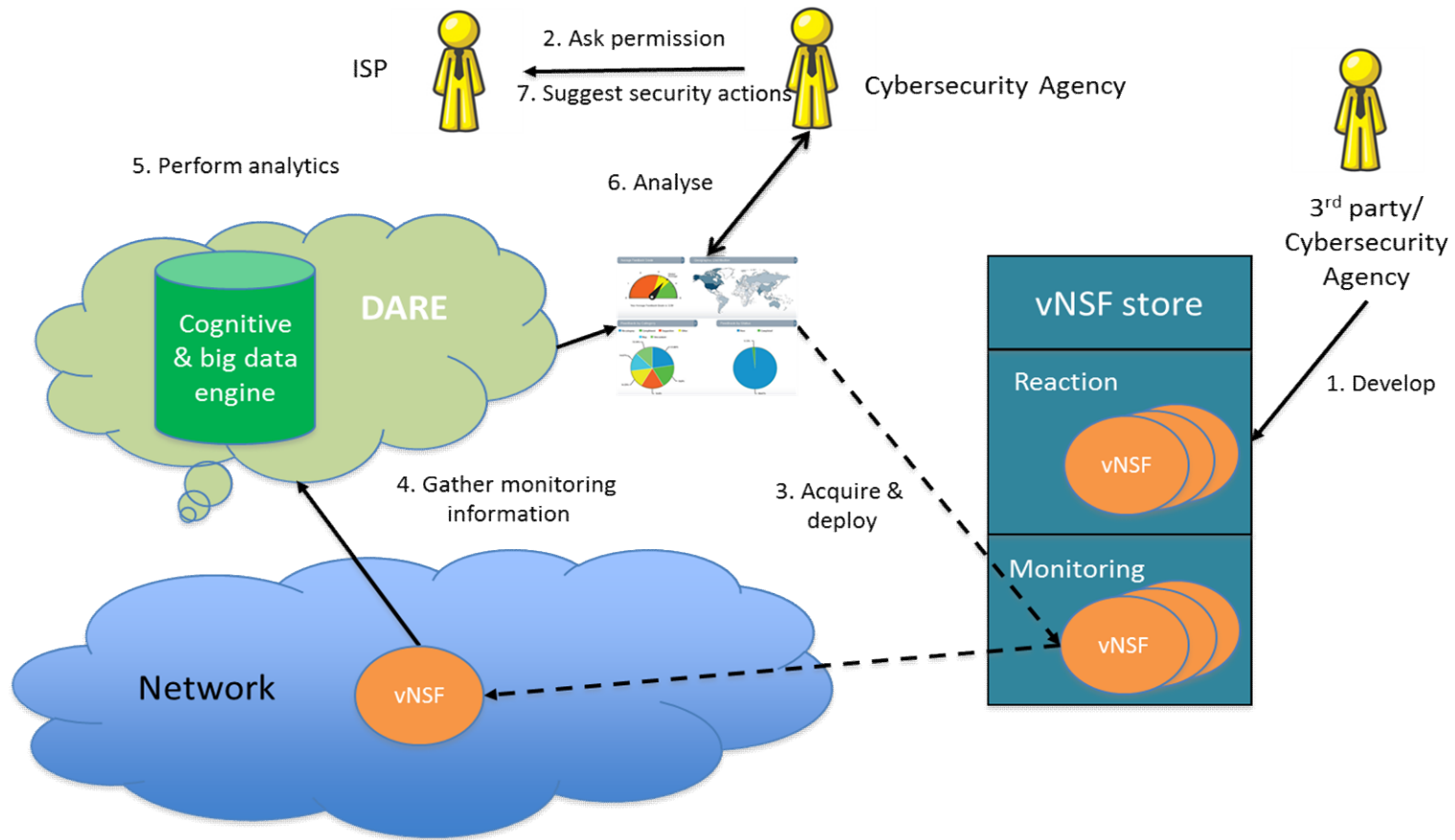




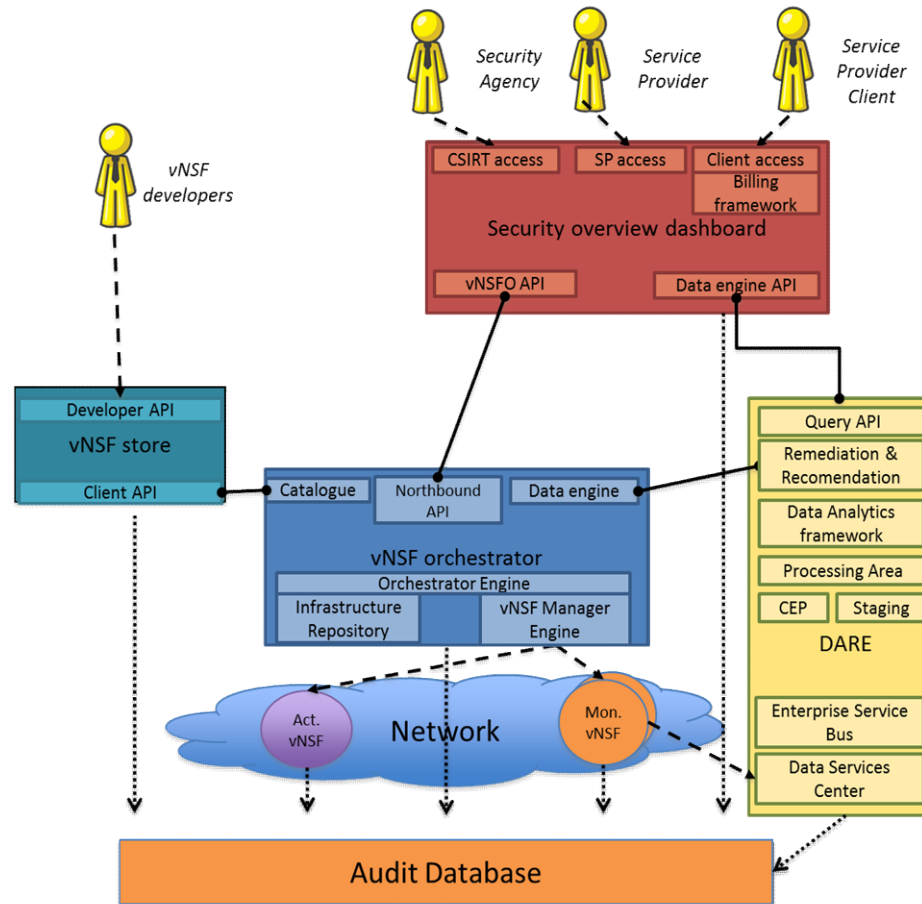
# Use-case 2: An ISP providing SecaaS



# Use-case 3: Contributing to national, European and global security



# Technical Architecture

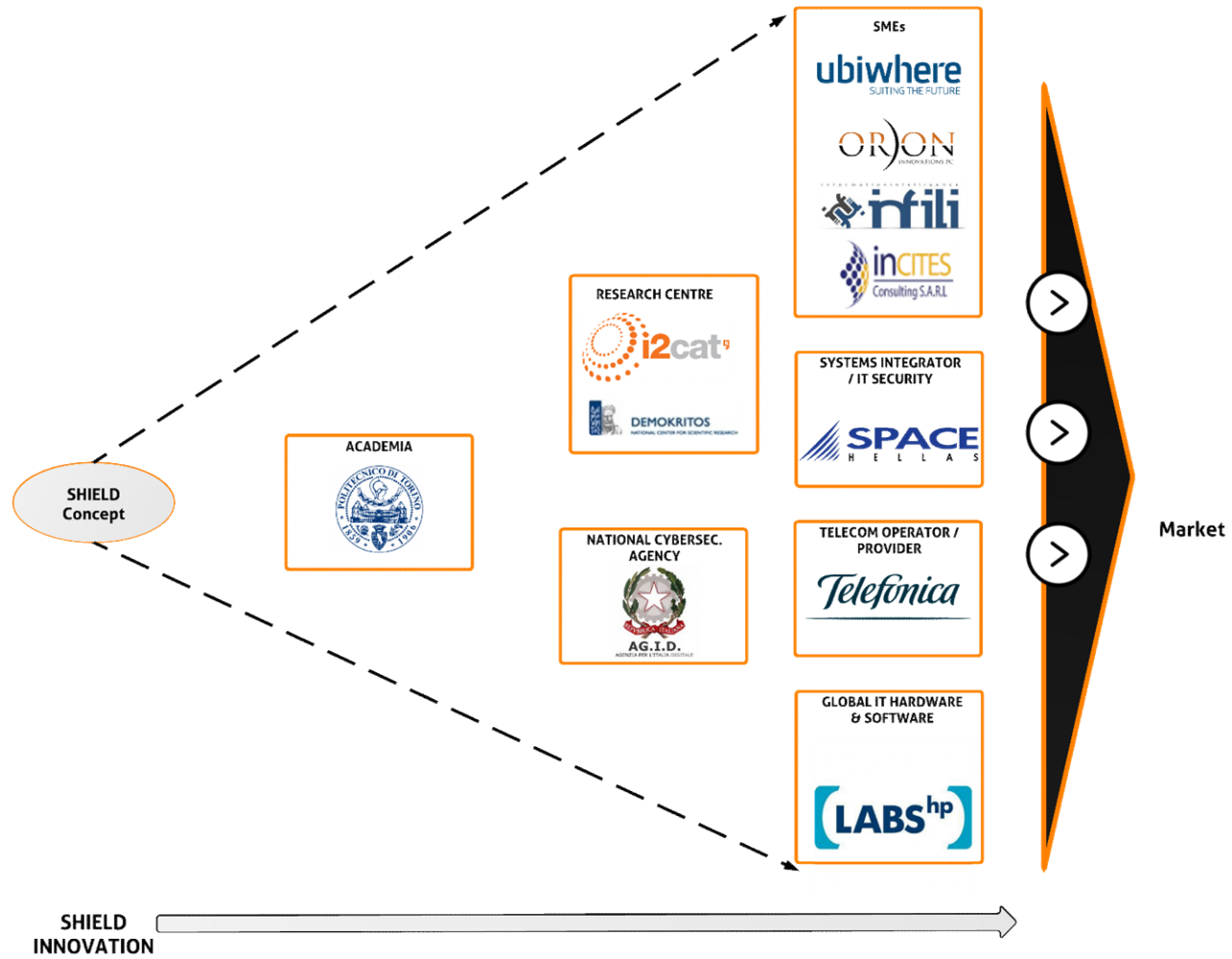


# Interested Stakeholders

---

- Telecom operators / ISPs
  - Enhancing and protecting their infrastructure with VNF support and with the SHIELD NFV orchestrator and big-data engine.
  - Increasing reusability of the virtual infrastructures, leading to resources and cost savings.
  - Possibility to offer SecaaS to their clients.
- ICT technology platform vendors and integrators
- Technology based SMEs
  - Fast neutralization of threats.
  - Possibility to hire SecaaS tailored to its needs.
  - Possibility to develop and sell new vNSFs.
- Public cybersecurity agencies
  - Access to data in a fastest way.
  - Easy to deploy security control mechanisms.
  - Research on attackers behaviour.
  - Tools to analyse data and react faster to threats.

# Consortium



# Numbers of SHIELD

---

- 1 Innovation Action
  - 5 Components (TRL 6 and above)
- 11 partners
  - 2 Research centres
  - 1 University
  - 1 Public Cybersecurity Agency
  - 3 Companies
  - 4 SMEs
- 3 LoS
  - CESICAT
  - INCIBE
  - Apfutura
- 6 WP
  - 1 Project Management
  - 1 Requirements
  - 2 Developing
  - 1 Integration and experimentation
  - 1 Exploitation
- 30 Months
- 4.7 M Budget
  - 3.6 M EC contribution



# Conclusions

---

- Cybersecurity is nowadays very related to Big Data, from cryptography to high-level solutions.
- Cybersecurity put the focus on some aspects regarding Big Data
  - Security of the infrastructure,
  - Security in every step of the Big Data technology,
  - Event based systems.
- Digital Society calls are a bit different from ICT calls.
  - Focus must be set in societal benefits.
  - Ethical aspects must be addressed.
- Can Telco BDVA subgroup lead the relation with cybersecurity PPP?
- Collaboration is the key!

