



ITEA international customer  
& end-user workshop  
**CYBER SECURITY**

# ITEA Cyber Security customer workshop feedback

# ITEA customer workshop on Cyber Security



## Participants [1/2]

- Organisation committee     
- Customers        
       
 
- Ambassador Digital Affairs 
- Industry technology providers   



# ITEA customer workshop on Cyber Security

## Participants [2/2]

- SME Technology providers



## Building trust

Any business requires trust between the stakeholders to be fluid and efficient. The digital transition strengthens the agility, fluidity and efficiency of the business, but all these advantages can be destroyed if we suffer too much from attacks. It requires to react collectively to the attacks because the attackers have a very fruitful business which allows them to invest massively to attack.

- **Maturity model** to trust a company
  - Security rating
  - Risk identification and selection - central to security by design
  - Bases for investment on security
  
- **Cyber Security Quality assurance** to trust a product service requires:
  - An agreed **maturity model**
  - Compliance rules per sector
  - Transparency
  - Operation aspect of the system / product
  
- **Risk awareness**
  - Methods for risk analysis to transform “risk” in a value of money
  - Automated tools to identify the risks are needed



- Business is very often reorganised around multitenant platforms → “Bubble of security & trust”
- Information about security attacks in a secure way → Methodology to define classification of information to protect
- We need to create communities of trusted defenders → Security maturity level definition and framework

- Any security requires to define a territory to protect;
- boundaries not aligned with the legal environment → definition and protection when sometimes borders of the IT system to secure are rather fuzzy

How to ensure security when the process to secure is real time →

- Reactiveness of security management?
- Multi-edge cloud architecture pushes the cloud closer to the end users to ensure better latency, but it generates new challenges for security
- How to handle latency constraints as security usually introduces overhead?



# Cyber Security customer challenges

## Heterogeneous legacy security tools management



- CSOs are confronted to numerous security tools
  - Connected with the flow of versions of the different softwares
- Continuous migration phase
- + Scarce expert resources





# Cyber Security customer challenges

## Security automation



- AI is required for automation and autonomous decision
- Challenge to control AI autonomous decisions not to impair the business model and the customer relationship; it requires explainable AI
- There is a problem of scale up



# Cyber Security customer challenges

## Secure components library

---



- Security is always a question of a system
  - but to build a secure system there is a demand of the customer for in-depth security
- Open secure commons



- Very often security = blocking access
  - But business = more and more agility and cooperation
  - Plus, when security makes system less easy to use = users bypass it
  - 60% of the attacks are from insiders
- Security usability = easier user life and to ensure security itself:
- Integrate privacy inside
  - Share data sets with good privacy level
  - Ensure simple but trusted right management



# Cyber Security customer challenges

## Internal security rules violation



- Many industries must respect some compliance rules, but employees lazy
- Tracking of rules (use case presented by Yapi Kredi Bank)



# Cyber Security customer challenges

## Strategic autonomy



- How to use a foreign technology while controlling the game
- E.g. use foreign cloud providers → protect access to hypervisor



# Cyber Security customer challenges

## Post Quantum computing cryptography



- Quantum computing will break the traditional asymmetric cryptographic model
  - It can arise sooner than forecasted
- Test and choose some new cryptographic models at the European level
- + transition plan





ITEA international customer  
& end-user workshop  
**CYBER SECURITY**

Stay tuned to the  
customers' demands