



# CYBER Security InSURance — A Framework for Liability Based Trust

Panos Chatziadam

FORTH-ICS

[panosc@ics.forth.gr](mailto:panosc@ics.forth.gr)





<https://cybersure.eu>

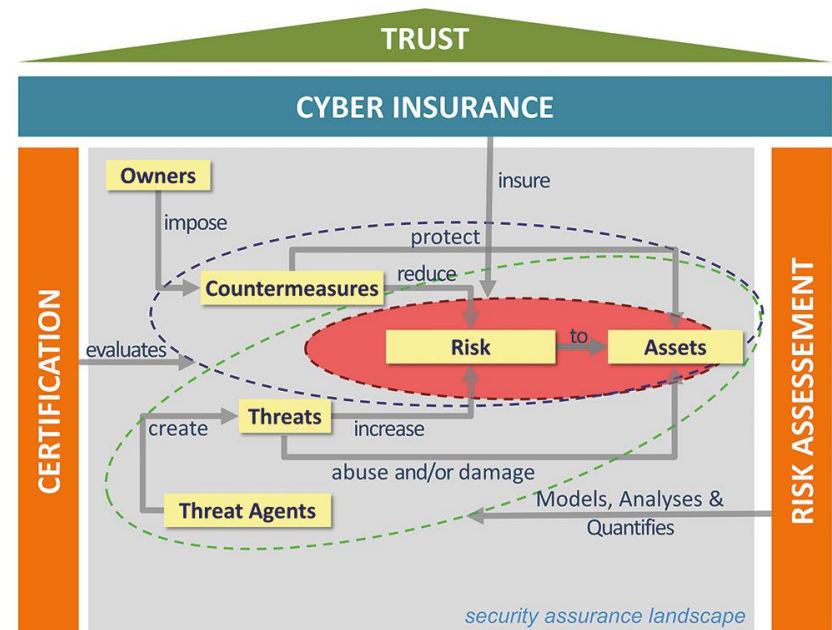
Call: H2020-MSCA-RISE-2016

GA number: 734815

Budget: €1,647,000

Duration: 4 years\*

Consortium: 3 industrial and 3 academic partners



CITY UNIVERSITY  
LONDON



cablenet





## Motivation

- Lack of tools to automate Cyber Risk assessment
- Lack of tools to monitor and Assess Cyber-security status
- Lack of tools to provide automated insurance policy compliance and ongoing updates
- Cyber-insurance and certification are either in isolation or in a manner that are not fully integrated and with no automation
- Cyber insurance policies require the existence of certificates, that are static and do not rely on operational evidence for the relevant systems and services

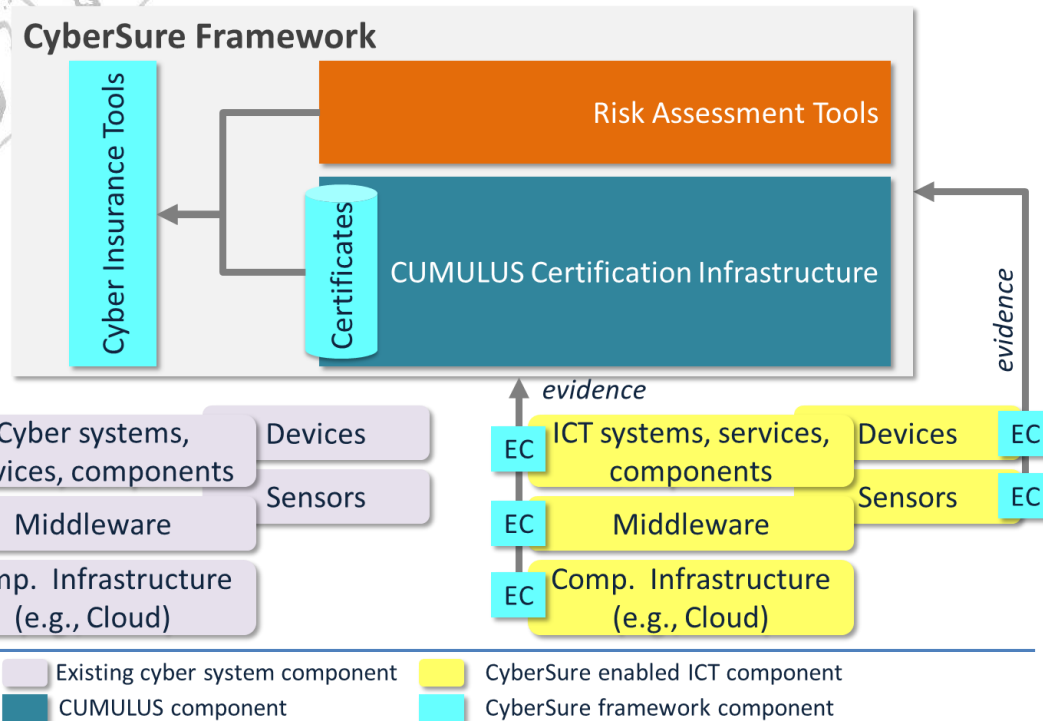




## Objectives

- Collaboration and Knowledge Exchange between the researchers
- Develop a framework for creating and managing Cyber Insurance Policies for cyber system by utilizing:
  - SOA continuous certification infrastructure (tools) for cloud services developed by the EU project CUMULUS at CITY
  - RM tool created by NIS and enhanced by CNR's NESSOS risk management methodology
  - Insurance management tools from Hellas Direct
- Create conditions for improving cyber insurance practice, the trustworthiness of cyber systems and commercializing the use of the CyberSure platform and framework
- Demonstrate the use of the CyberSure framework in real world trials in the areas of e-health and cloud services
- Demonstrate system prototype in a simulated laboratory environment







## Cyber-Insurance process

- **Baseline risk analysis:** Risk assessment methodologies and tools will support the early analysis and specification of risk models
- **Certification:** Generation of executable cyber system certification models and use them to carry out assessments of the soundness and the effectiveness of the countermeasures used for mitigating risks
- **Comprehensive risk assessment:** The certificates and/or the operational evidence generated by certification should provide inputs to a subsequent comprehensive assessment of risk that may be required for formulating and pricing cyber insurance policies
- **Cyber insurance policy management:** This phase covers the activities of managing cyber insurance policies, i.e. policy creation, pricing and updating and claim handling





## Risk Assessment

- Risk assessment for Cyber Insurance – Provide practical Risk Assessment targeted at organizations providing Cyber Insurance. This leads to the enrichment of the Cyber Insurance sector via the application of Risk Assessment methodologies and innovative techniques applied to Cyber Services.
- Evidence-based Risk Assessment – Dynamic and automated Risk Assessment evidence collection as opposed to manual testimony-based Risk Assessment (remove the human factor). This leads to the improvement of insurance setup process and policy identification through objectives and measurable assessments of the degree of reliability.
- Dynamic Risk Assessment – Risk Assessment is continuously calculated based on the Risk Level obtained by the collected evidence. This leads to dynamic semi-automated adaptation of the insurance policy based on the evidence collected.





## Goals

- Develop an innovative framework to support the creation and management of cyber insurance policies and offering a sound liability basis for establishing trust in cyber systems and services
- This framework will be supported by a platform of integrated tools enabling:
  - the dynamic certification of security and privacy properties of cyber systems and services that need to be insured
  - the dynamic estimation of security and privacy risks for such systems and services
  - the development, monitoring and management of cyber insurance policies for these systems and services based on a) and b)
- The platform developed will be market ready and validated through demonstration in operational environments at TRL-7\*







## Business Impact

- Cyber Insurers
  - Provision of a comprehensive approach and platform for creating, monitoring and adapting cyber insurance policies therefore providing Cyber insurance policies customised to the needs of individual customers and their organizational risk assessment
  - Dynamic and continuous risk assessment will lead to more thorough and accurate basis for monitoring cyber insurance policies and therefore a reduction of risk and cyber insurance management costs and consequently policy premiums
- Cyber system providers
  - Improve security through the provision of automated risk management and S&P assessment and certification services
  - Incentivise service providers to improve their security according to reference security standards and benchmarks, in order to reduce their insurance premiums
  - Establishment of liability through the undertaking of cyber insurance policies





**THANK** you!

