# a Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020

SECONDO

"SECONDO: An innovative platform for estimating cyber insurance premium"

## InsurTECH 2021

Prof. Christos Xenakis

Project Coordinator, University of Piraeus

Department of Digital Systems

Greece

European Commission | Horizon 2020 European Union funding for Research & Innovation

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 823997.

# SECONDO

# Project Overview
# SECONDO consortium

Project Information

SECONDO

Grant agreement ID: 823997

Status

Ongoing project

Start date

1 January 2019

End date

31 December 2022

Funded under

H2020-EU.1.3.3.

Overall budget

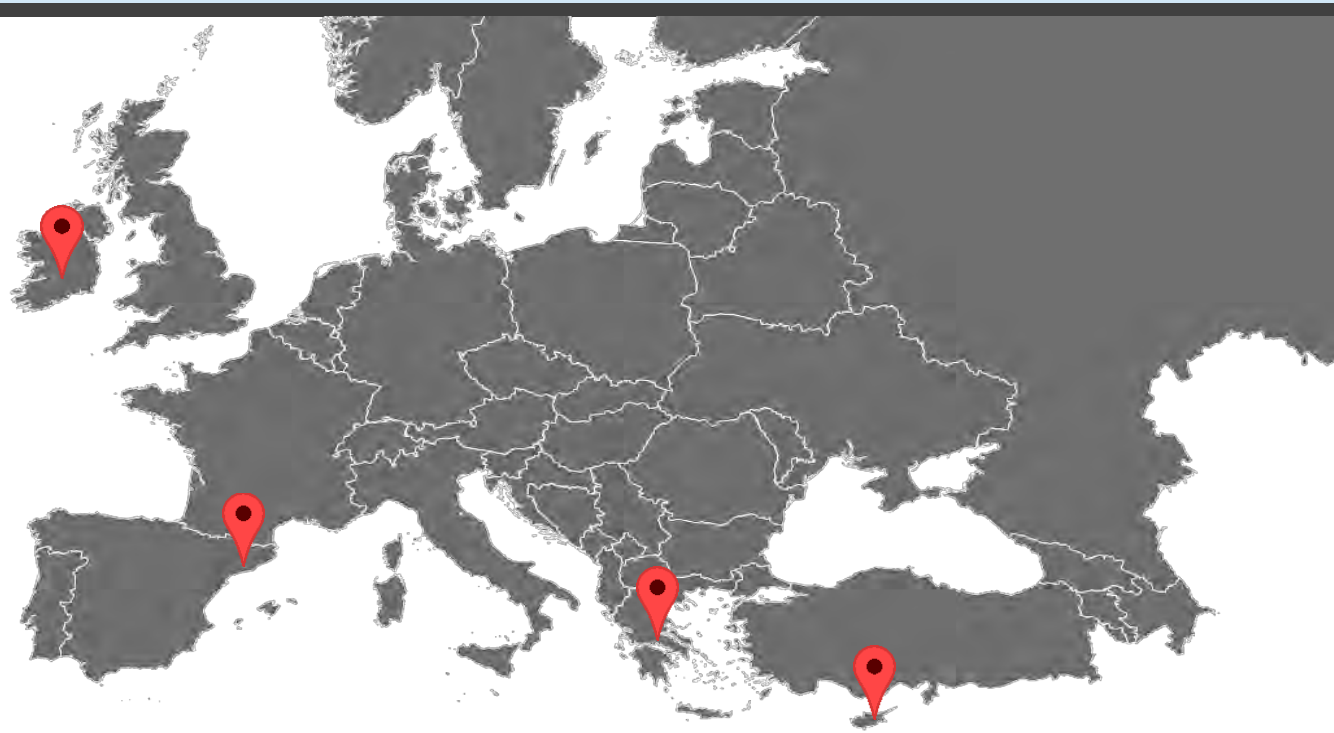
€ 1 600 800

EU contribution
€ 1 600 800

Coordinated by

UNIVERSITY OF PIRAEUS RESEARCH CENTER

Greece



UNIVERSITY OF PIRAEUS

UNIVERSITY OF SURREY

Cyprus University of Technology

UBITECH ubiquitous solutions

CROMAR INSURANCE BROKERS LTD

LS TECH

FOGUS INNOVATIONS & SERVICES

UNIVERSITY of GREENWICH

# Motivation: Cyber Security Threats

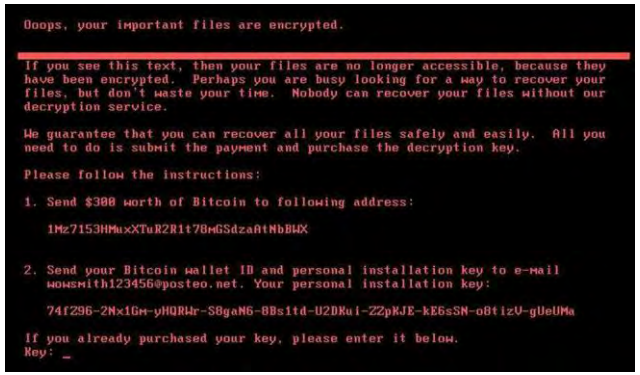
- Since **COVID-19**, the US FBI reported an increase of **300%** in reported **cybercrimes**.
- Cybercrime **damage** may cost the world **$6 trillion annually** by 2021.
- **67%** increase in **security breaches** in the last five years.
- Cost of **ransomware** to businesses will top **$20 billion** in 2021.
- A **ransomware** attack every **14 seconds**.
- **Social media logins** is available for **$2.73 each** in the Dark Web
- For sale in the Dark Web **20 billion passwords & emails**

**Data** is the new **oil** of the **21st century**

https://blog.s4rb.com

# Cyber Attacks

- **NotPetya, Worldwide, 2017**
  - **Ransomware**
  - **$300** to regain access on each computer
  - Mondelez:$100M
  - Maersk:$300M
  - Merck:$800M
  - **Damage of more than 10 Billions**
  - **Insurers had denied claims**




- **Marriott Cyberattack, 2018**
  - Since 2014
  - **500M** guest records exposed
  - Reimbursements: **$71M**
  - **$120M** fined under the GDPR

- **Shen-attack scenario**
  - Ransomware hypothesis
  - Cost of Cyber Attack on Asia-Pacific Ports Could Reach **$110B**.
  - **92%** of all losses resulting from a cyber attack would not be insured.


- **Simon Weckert Causes Google Maps "Traffic Jams" By Carrying 99 Cell Phones, February 2020**

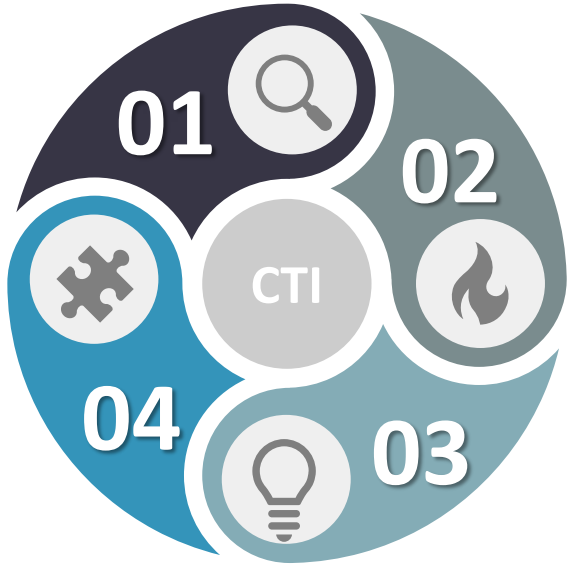
# Cyber Threat Intelligence

## Acquire Data

- **Internal Sources**
- **External Sources**
  - **Open source** intelligence
  - **Social media** intelligence
  - **Human intelligence**
  - **Dark Web**

## Continuous Risk Monitoring

- Assess on a continuous basis the **risk levels** and the **performance of the implemented cyber security controls**




## Analyze Data

- **Artificial intelligence**: make **predictions** and **extract insights** and **patterns**
- **Data analytics:** analyze raw data to **make conclusions**
- **Machine learning**: **predict** and **find representative values** for the missing data

## Intelligence

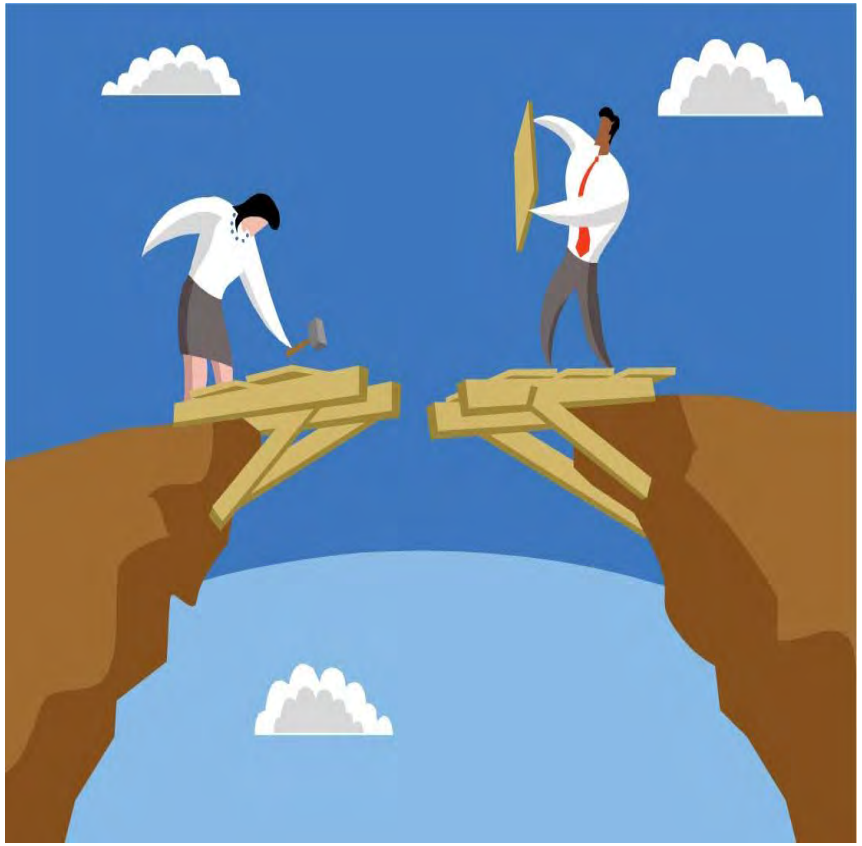
- **Detect** threats
- **Understand** & **Evaluate** organization's status
- **Response and prepare** the organization's future actions
  - **Mitigate Risk**
  - **Risk Transfer**

# Scientific Challenges

**"85% say Threat Intelligence is important for a strong security posture**
**but 41% say they have not made progress in the effectiveness of Threat Intelligence data."**
1000 IT&Security Companies, 2019, Ponemon institute.

- Proper team to manage CTI activities
- Allocate adequate budget
- Data sources
- Threat Intelligence Sharing
  - Validation
  - Quality
  - Speed
  - Correlation


- Security Team's understanding
  - Motivation
  - Infrastructure
  - Awareness
  - Methods
- Integrate CTI with organization
  - Endpoint detection and response
  - Security information and event management – SIEM
  - Firewalls
  - Incident Management Systems
  - Intrusion Detection Systems – IDS

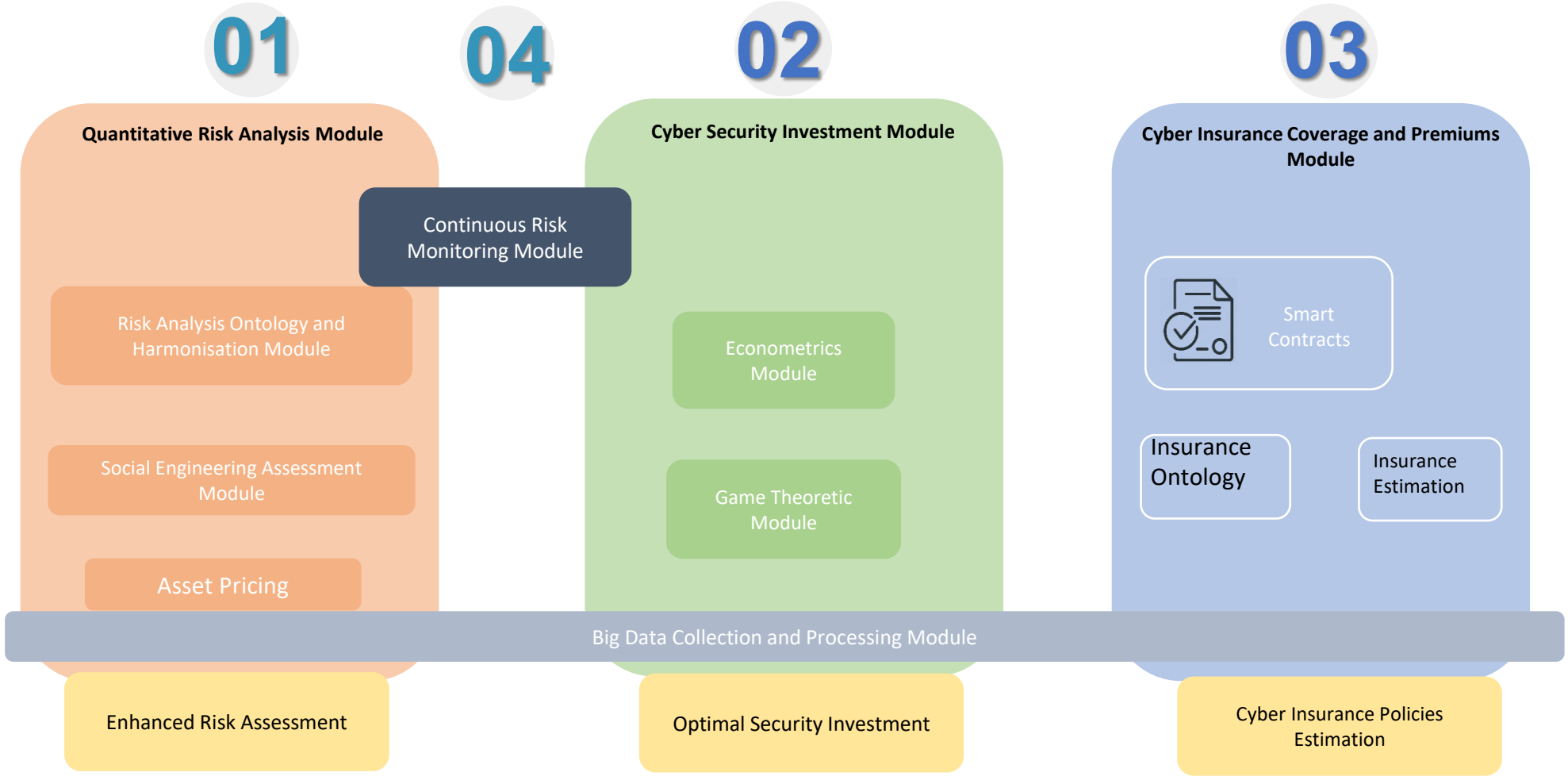


**SECONDO** proposes an **Economics-of-Security-as-a-Service (ESaaS) platform** that encompasses a comprehensive **cost-driven** methodology for:

- estimating **cyber risks** based on a **quantitative** approach (on both **technical** and **non-technical** aspects)
- recommending **optimal investments** in cyber security for efficient **risk management**
- determining the **residual risks** and estimating the **cyber insurance premiums**

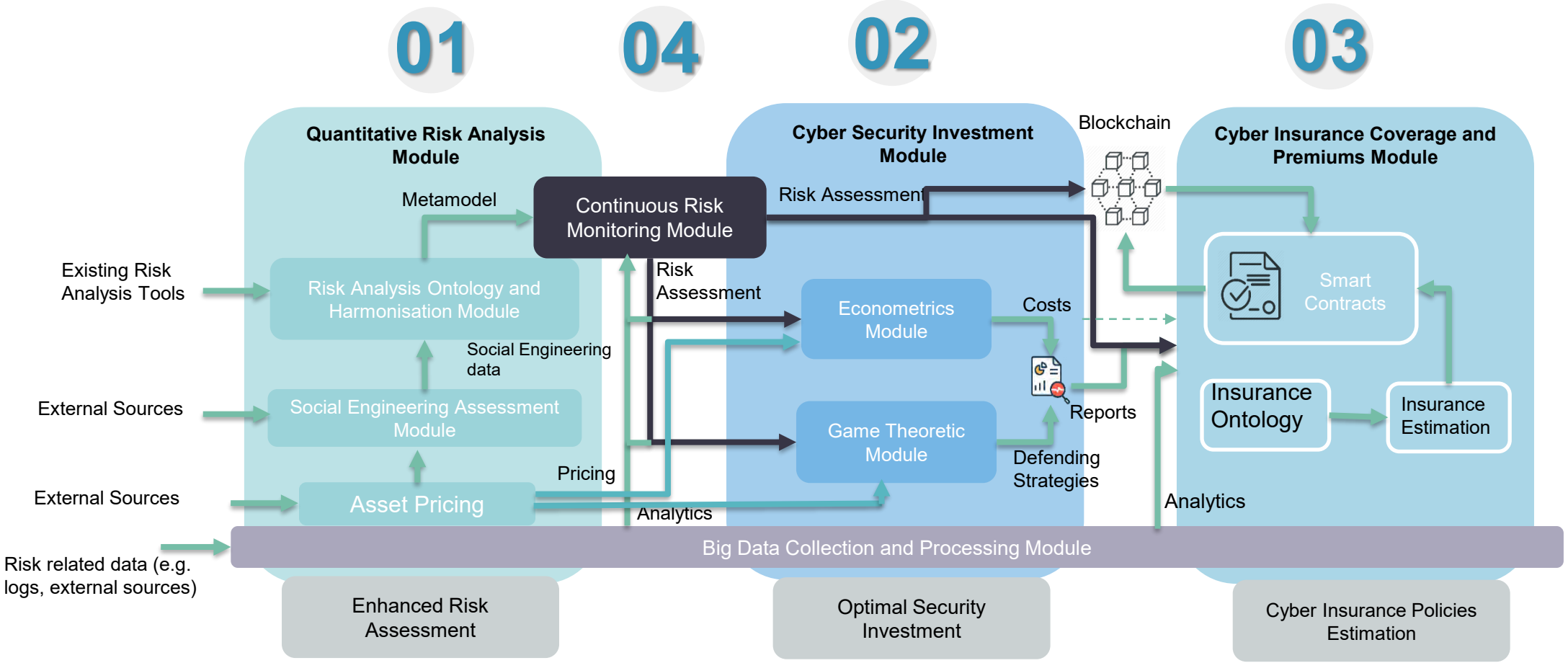
# SECONDO

# The SECONDO platform



# SECONDO

# The SECONDO platform



# SECONDO

# The SECONDO platform

## Acquire Data

- Phishing
- SIEM
- Log files (Firewall, IDS)
- Social Media
- ELK stack
- Python
- Apache


## Analyze Data

- Python
- Pandas Library
- ELK stack
- CORAS Method
- Nash Equilibria

## Continuous Risk Monitoring

- OLISTIC Enterprise Risk Management
- Blockchain
- Ethereum private blockchain

## Intelligence

- Econometric Methods
- Optimal Decisions
- Premiums and Coverages
- Privacy-preserving smart contracts
- Solidity

# Architectural Main Goals

- **Architectural Main Goals**
  - Transparency.
  - Trust.
  - Privacy.
  - Fraud deterrence.
  - Lower costs.
  - Faster response.
  - Optimal decisions.
  - Optimal Risk Assessment.

# SECONDO Challenges

1. Optimal Risk Assessment
2. Smart Contracts
3. Cyber Threat Mitigation
4. Predict Attacking Scenarios
5. Adapt to new changes and needs

6. Adjust to organization topology
7. Accurate Data
8. Continuous Risk Monitoring
9. Detect-Prepare-Prevent-Protect
10. Reduce cyber security budget


SECONDO

Prof. Christos Xenakis
University of Piraeus
xenakis@unipi.gr