SHARE MORE THAN TECHNOLOGY

proximus NXT
cybersecurity

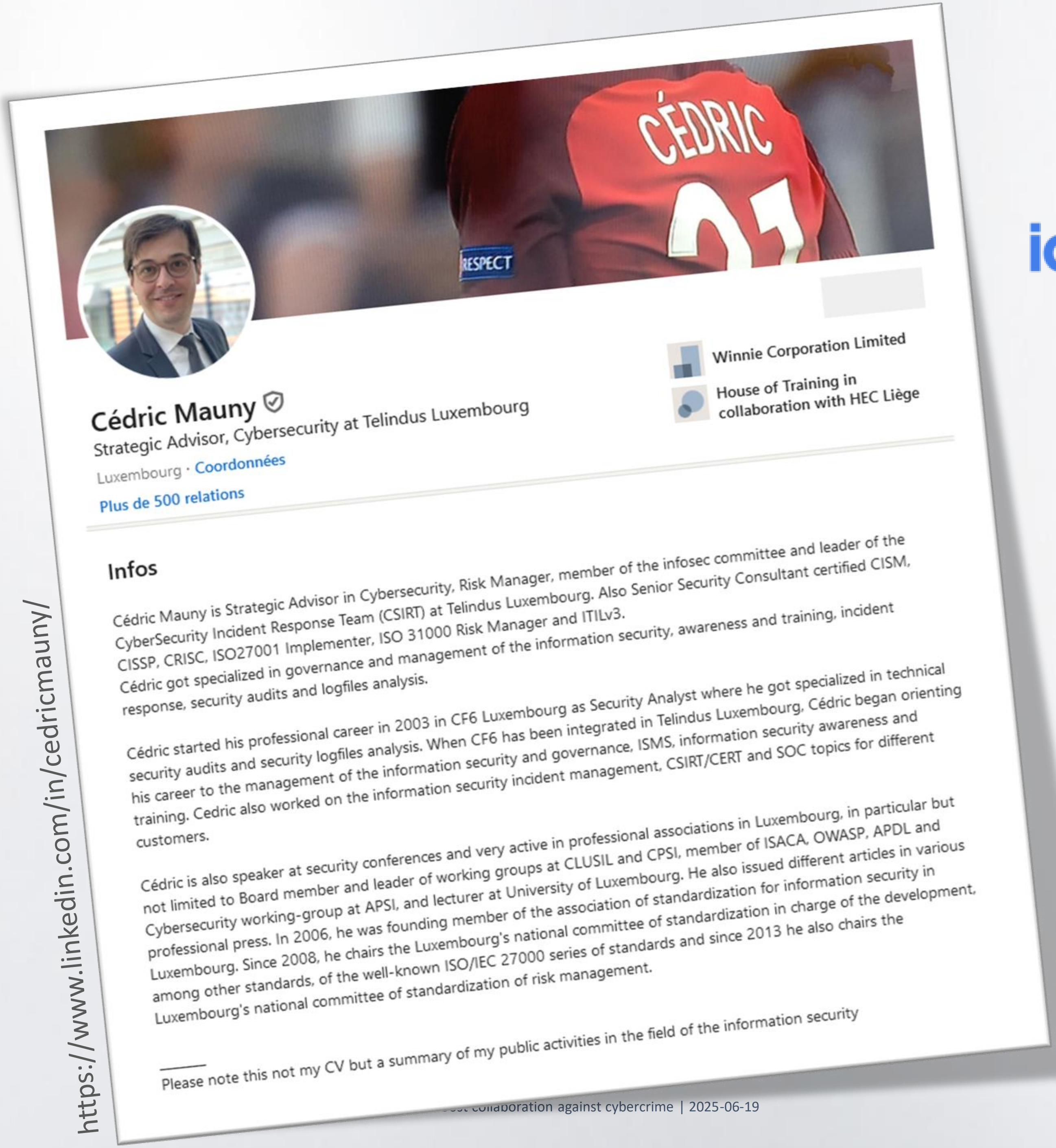
BSIDES LUXEMBOURG
https://bsides.lu

Remove barriers to data sharing to boost collaboration against cybercrime

2025-06-19 from 16h to 16h25

Cédric Mauny
Strategic Advisor, Cybersecurity

Who am I?



Cédric Mauny

Strategic Advisor, Cybersecurity at Telindus Luxembourg

Luxembourg · Coordonnées

Plus de 500 relations

Winnie Corporation Limited

House of Training in collaboration with HEC Liège

Infos

Cédric Mauny is Strategic Advisor in Cybersecurity, Risk Manager, member of the infosec committee and leader of the CyberSecurity Incident Response Team (CSIRT) at Telindus Luxembourg. Also Senior Security Consultant certified CISM, CISSP, CRISC, ISO27001 Implementer, ISO 31000 Risk Manager and ITILv3.
Cédric got specialized in governance and management of the information security, awareness and training, incident response, security audits and logfiles analysis.

Cédric started his professional career in 2003 in CF6 Luxembourg as Security Analyst where he got specialized in technical security audits and security logfiles analysis. When CF6 has been integrated in Telindus Luxembourg, Cédric began orienting his career to the management of the information security and governance, ISMS, information security awareness and training. Cedric also worked on the information security incident management, CSIRT/CERT and SOC topics for different customers.

Cédric is also speaker at security conferences and very active in professional associations in Luxembourg, in particular but not limited to Board member and leader of working groups at CLUSIL and CPSI, member of ISACA, OWASP, APDL and Cybersecurity working-group at APSI, and lecturer at University of Luxembourg. He also issued different articles in various professional press. In 2006, he was founding member of the association of standardization for information security in Luxembourg. Since 2008, he chairs the Luxembourg's national committee of standardization in charge of the development, among other standards, of the well-known ISO/IEC 27000 series of standards and since 2013 he also chairs the Luxembourg's national committee of standardization of risk management.

———

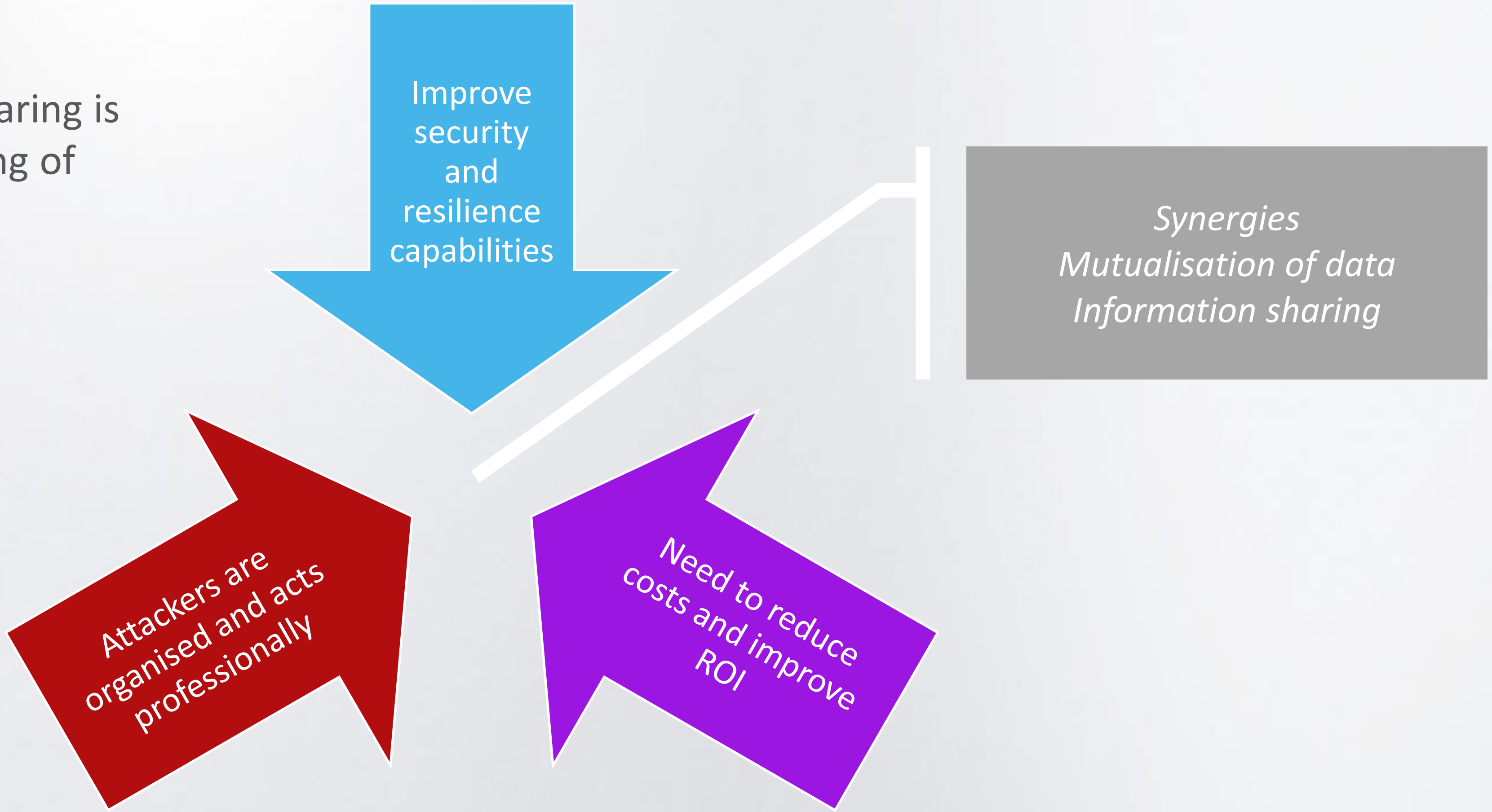
Please note this not my CV but a summary of my public activities in the field of the information security

https://www.linkedin.com/in/cedricmauny/

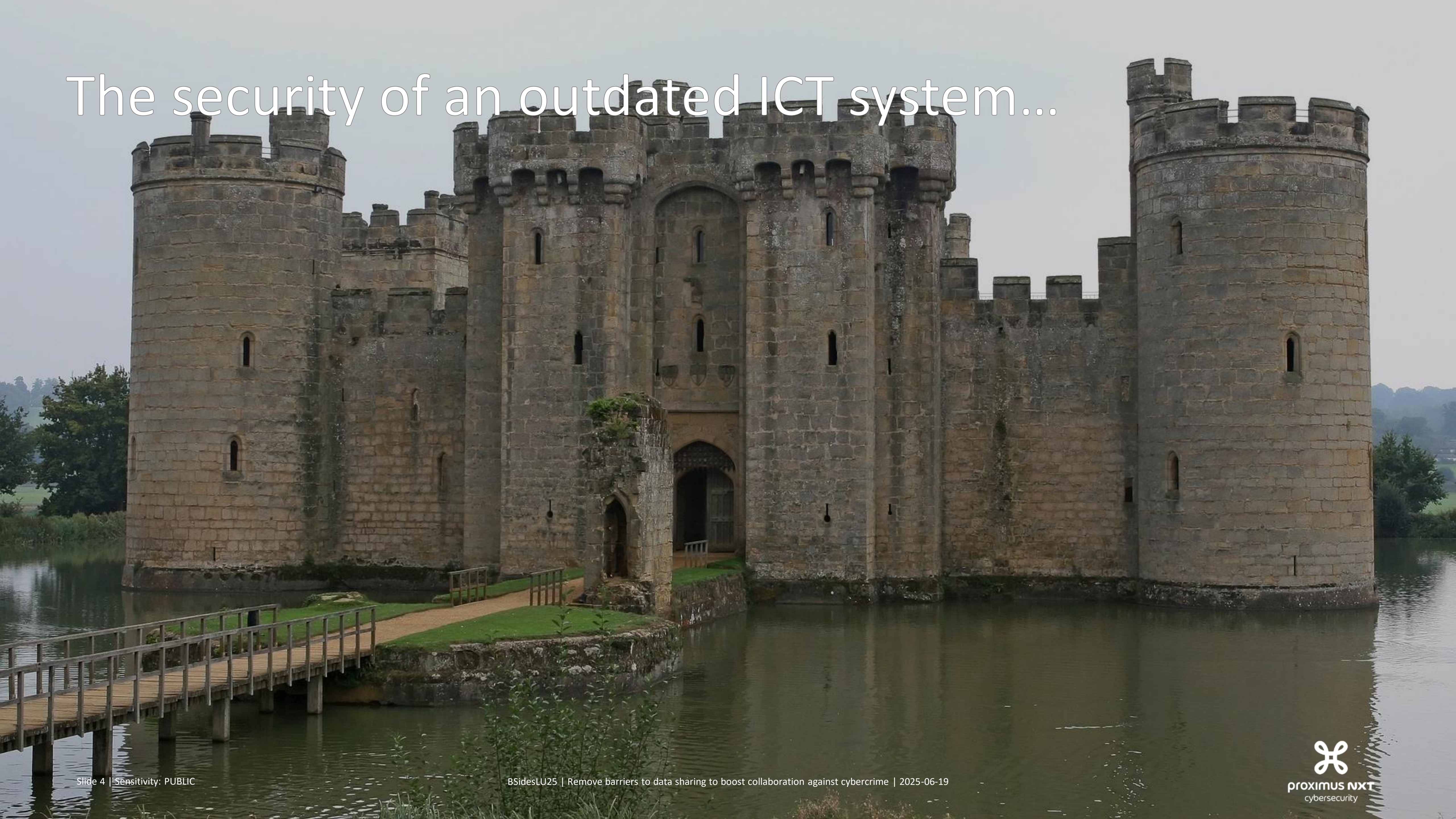
Fighting cybercrime needs synergies

Addressing a triple-challenge

In cybersecurity, information sharing is crucial for a better understanding of threats and to prevent attacks


Improve security and resilience capabilities
Attackers are organised and acts professionally
Need to reduce costs and improve ROI
Synergies
Mutualisation of data
Information sharing

The security of an outdated ICT system…



… relies on an outdated way to manage risks

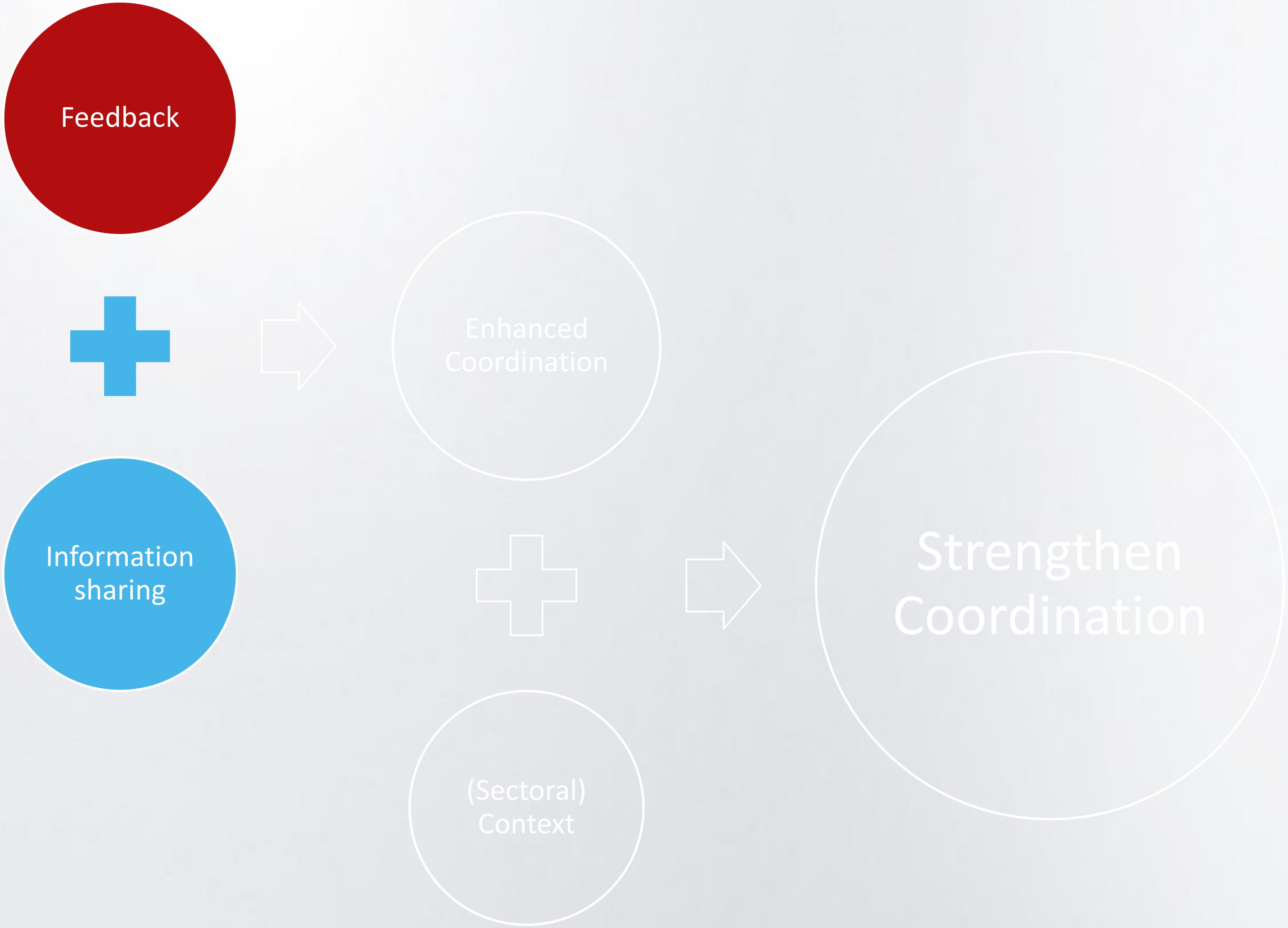
See no evil *Hear no evil* *Speak no evil*

It’s now time to adopt a ~~new~~ model…

… which requires to adapt existing practices of risk monitoring…

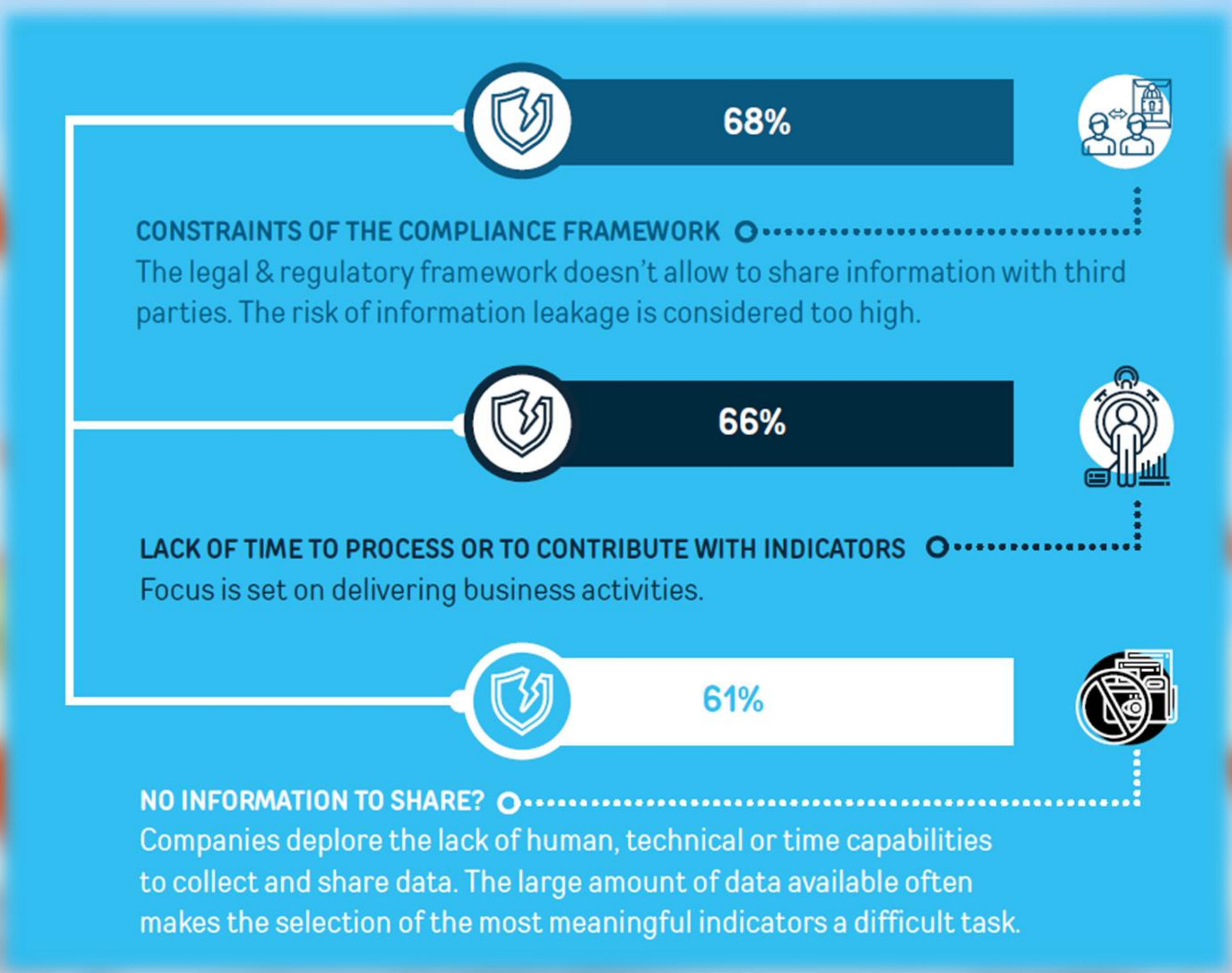
… and sharing collected information to enforce global protection

How to *enhance* coordination?



Obstacles to information sharing are known

Obstacles to information sharing are known



68%

CONSTRAINTS OF THE COMPLIANCE FRAMEWORK
The legal & regulatory framework doesn't allow to share information with third parties. The risk of information leakage is considered too high.

66%

LACK OF TIME TO PROCESS OR TO CONTRIBUTE WITH INDICATORS
Focus is set on delivering business activities.

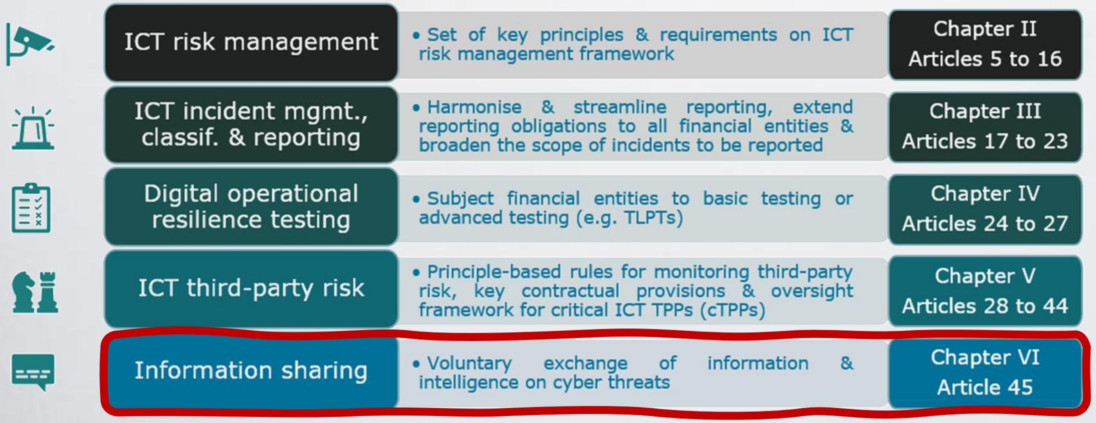
61%

NO INFORMATION TO SHARE?
Companies deplore the lack of human, technical or time capabilities to collect and share data. The large amount of data available often makes the selection of the most meaningful indicators a difficult task.

TELINDUS CYBERSECURITY REPORT 2019 telindus

Constraints of the compliance framework as explanation for not sharing information?!

- **DORA**
  Digital Operational Resilience Act
- Applicable since 17th January 2025



ICT risk management	• Set of key principles & requirements on ICT risk management framework	Chapter II Articles 5 to 16
ICT incident mgmt., classif. & reporting	• Harmonise & streamline reporting, extend reporting obligations to all financial entities & broaden the scope of incidents to be reported	Chapter III Articles 17 to 23
Digital operational resilience testing	• Subject financial entities to basic testing or advanced testing (e.g. TLPTs)	Chapter IV Articles 24 to 27
ICT third-party risk	• Principle-based rules for monitoring third-party risk, key contractual provisions & oversight framework for critical ICT TPPs (cTPPs)	Chapter V Articles 28 to 44
Information sharing	• Voluntary exchange of information & intelligence on cyber threats	Chapter VI Article 45

https://www.cssf.lu/en/ict-and-cyber-risk-for-dora-entities/

- **NIS2**
  Network and Information Systems (Security) v2
- Applicable since 17 octobre 2025 (or not yet)

- Mandatory and voluntary information sharing and notification of information
- Article 29.2 from the Directive
  - *Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers.*
  - *Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared*

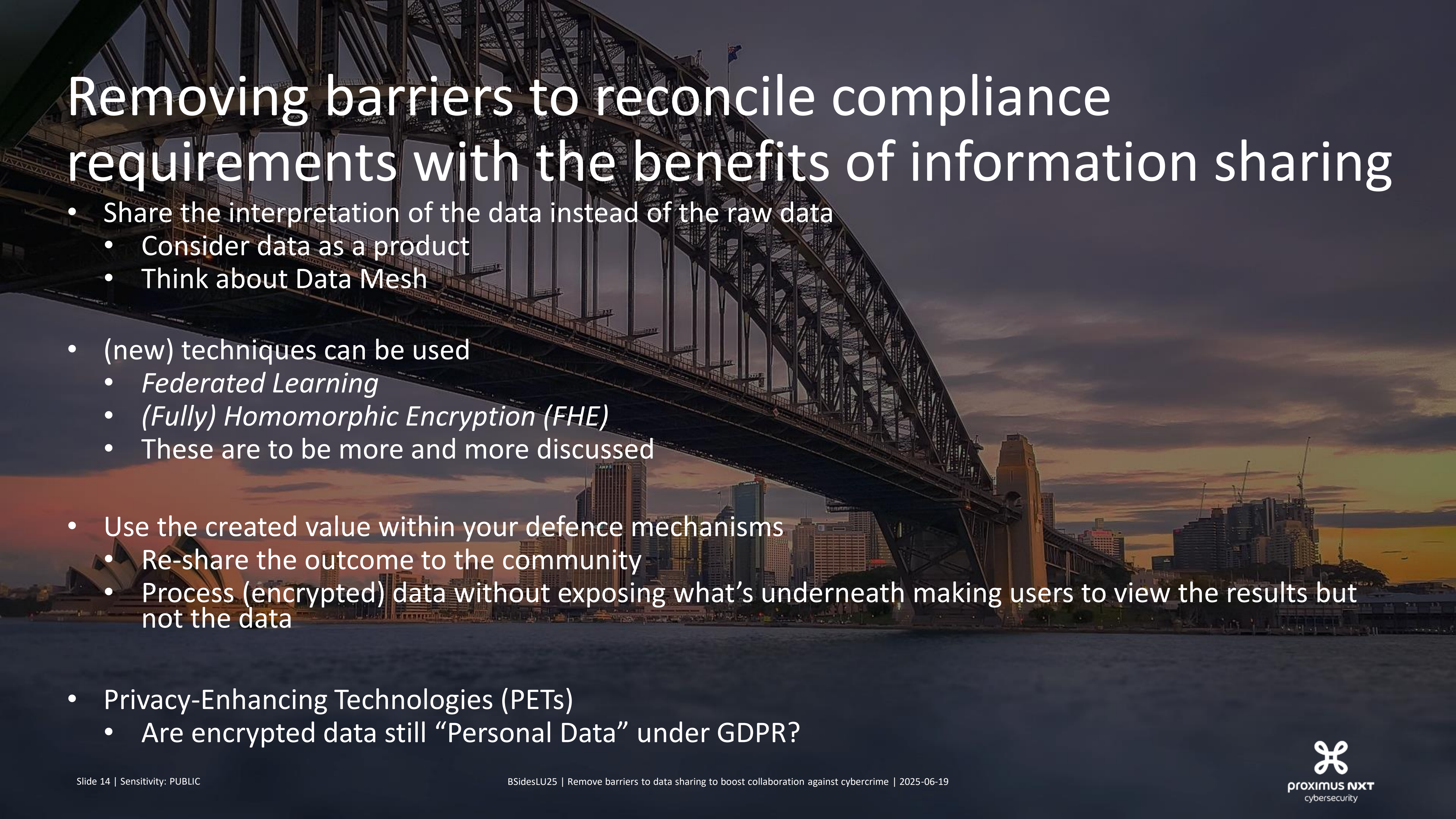
Remove barriers limiting information sharing between peers and competitors to globally improve the security posture of the Community

- Failures to be addressed
  - Coordination failure
    - Lack of cybersecurity cooperation to create threat intelligence capabilities limit capabilities of fighting cybercrime
  - Bilateral informational synergies only
    - Knowledge may be loss and advantages of sectoral approach may be reduced

- Why (not) using (new) mechanisms to address expressed limitation of information sharing
  - **Identify the key information** by asking to the people who create and manage the data from business perspective
  - **Maintain the confidentiality and privacy** when exchanging and processing data (by default, from a transparent manner)
  - **Spare resources** by mutualizing the learning phase of multiple AI models between different companies ("le moment IA" ;)
  - *Idea*
    - Leverage the capabilities offered by different (new?) technical mechanisms to enhance coordination between companies to show the value of data

- (side)Objectives
  - Improve market global detection capabilities
  - Sparing and sharing resources by pooling and combining data with peers (partners, competitors, …)
  - Get a view on the sectoral risks to improve the capabilities of informed governance when dealing with relevant cyber-risks / crisis that may disturb an economic sector
  - Preserve confidentiality of information in line with needs, expectations and regulations

- Outcome of the *idea* could be *something* (product/service) that support the setup of a collective intelligence while removing the traditional barriers of information sharing



Removing barriers to reconcile compliance requirements with the benefits of information sharing

- Share the interpretation of the data instead of the raw data
  - Consider data as a product
  - Think about Data Mesh

- (new) techniques can be used
  - *Federated Learning*
  - *(Fully) Homomorphic Encryption (FHE)*
  - These are to be more and more discussed

- Use the created value within your defence mechanisms
  - Re-share the outcome to the community
  - Process (encrypted) data without exposing what's underneath making users to view the results but not the data

- Privacy-Enhancing Technologies (PETs)
  - Are encrypted data still "Personal Data" under GDPR?

Data Mesh

- Too much centralisation of data reduce sharing opportunities and recognition of value of the data

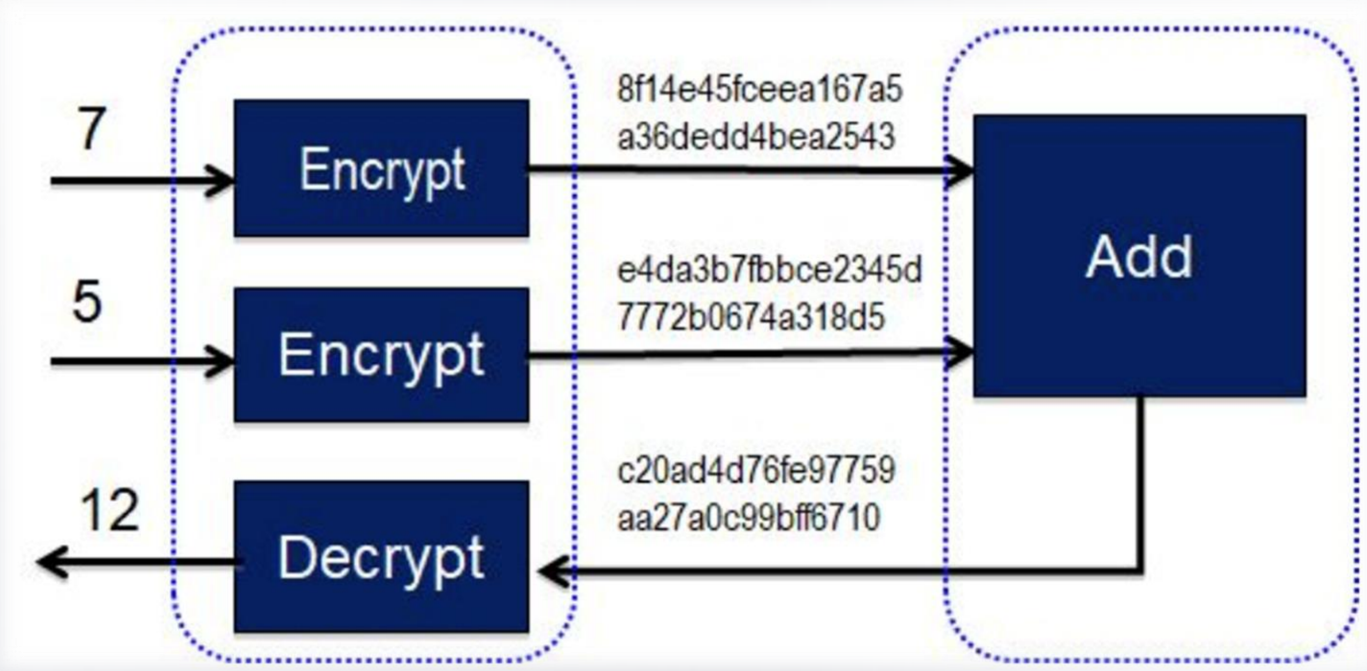
- Before: data is managed from a centralized point of view by a central team in a central Datawarehouse
- Then: Data Mesh is based on a decentralized data ownership and architecture, making individual teams responsible for their own data domains
  - The valuable data is managed by the team itself
  - The process of data is performed by the team itself
  - The sharing of data is managed by the team itself

- Data is not expected to be shared but the interpretation of data is expected to be
  → *Data-as-a-(security)Product*
  - Reduce the risk of data leakage as data by itself will not be shared
  - "Cybersecurity value of the data" is intended to be shared

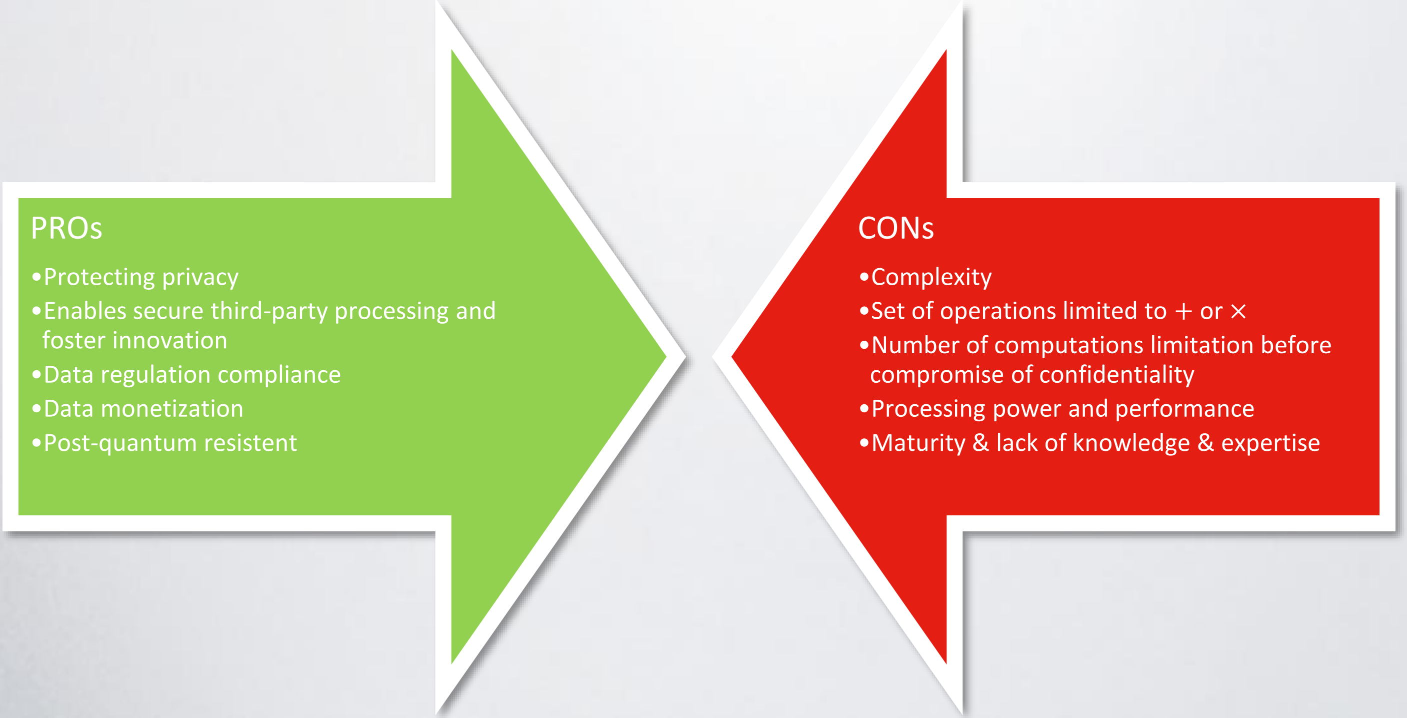
Homomorphic Encryption

- *Homomorphic encryption* is a method of encryption that allows computations and queries to be performed upon fully encrypted data, making it possible to analyze or manipulate encrypted data without decrypting it

- Limitations
  - Type of operations
    - Limited to + or ×
  - Number of computations
    - Before compromise of confidentiality
  - Performance and processing power



Homomorphic Encryption



PROs

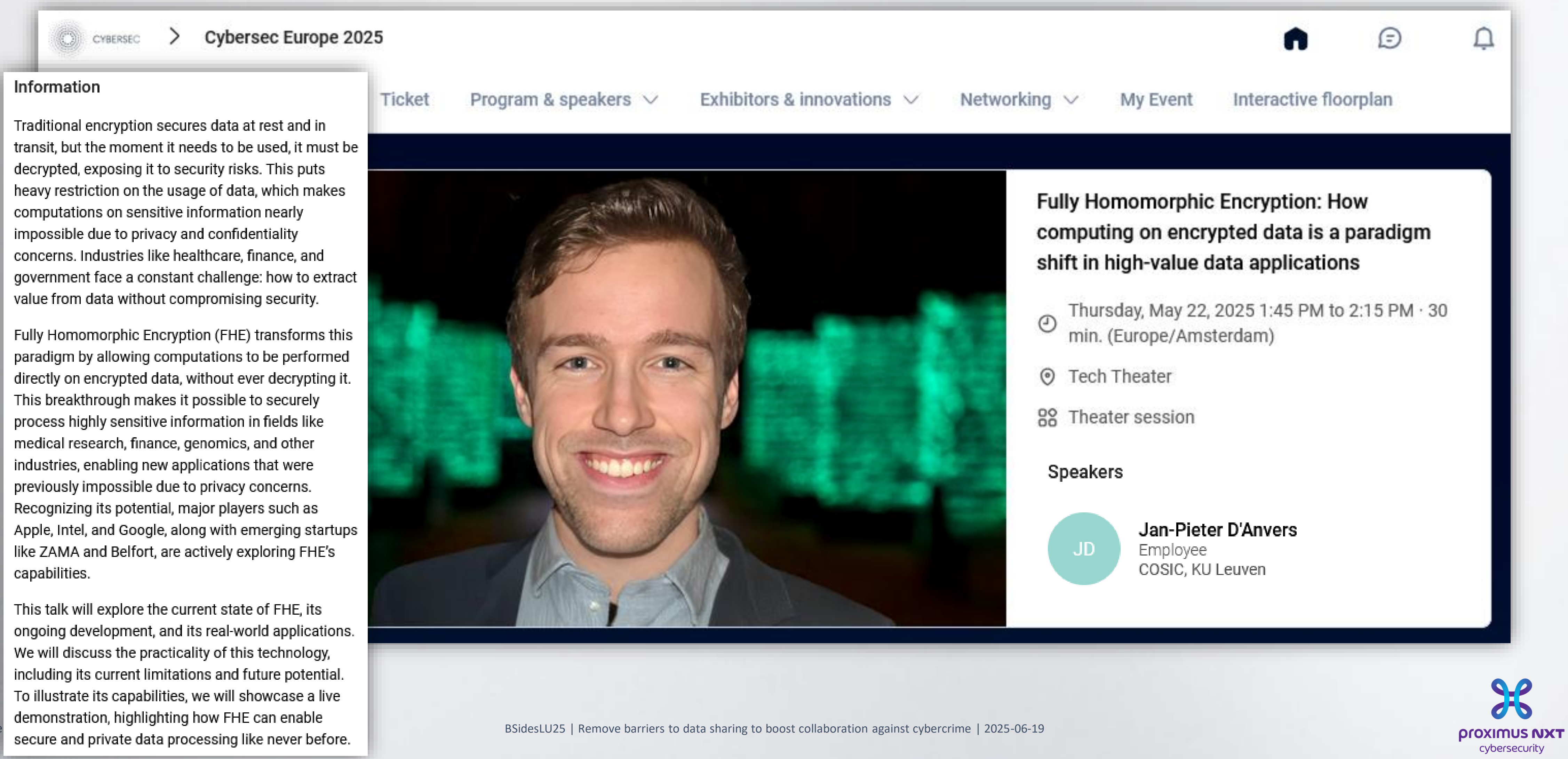
- Protecting privacy
- Enables secure third-party processing and foster innovation
- Data regulation compliance
- Data monetization
- Post-quantum resistent

CONs

- Complexity
- Set of operations limited to + or ×
- Number of computations limitation before compromise of confidentiality
- Processing power and performance
- Maturity & lack of knowledge & expertise

- Use-cases
  - Use-cases in which the direct users of a dataset (and those who use downstream applications) are trusted with all the sensitive information, but the compute environment, such as a public cloud, is not trusted with sensitive information
  - Securing Cloud Compute/Storage
  - Enabling Data Analytics
  - Electronic Voting

Fully Homorphic Encryption is (now) (will be) a thing



CYBERSEC > Cybersec Europe 2025

Information

Traditional encryption secures data at rest and in transit, but the moment it needs to be used, it must be decrypted, exposing it to security risks. This puts heavy restriction on the usage of data, which makes computations on sensitive information nearly impossible due to privacy and confidentiality concerns. Industries like healthcare, finance, and government face a constant challenge: how to extract value from data without compromising security.

Fully Homomorphic Encryption (FHE) transforms this paradigm by allowing computations to be performed directly on encrypted data, without ever decrypting it. This breakthrough makes it possible to securely process highly sensitive information in fields like medical research, finance, genomics, and other industries, enabling new applications that were previously impossible due to privacy concerns. Recognizing its potential, major players such as Apple, Intel, and Google, along with emerging startups like ZAMA and Belfort, are actively exploring FHE's capabilities.

This talk will explore the current state of FHE, its ongoing development, and its real-world applications. We will discuss the practicality of this technology, including its current limitations and future potential. To illustrate its capabilities, we will showcase a live demonstration, highlighting how FHE can enable secure and private data processing like never before.

Fully Homomorphic Encryption: How computing on encrypted data is a paradigm shift in high-value data applications

Thursday, May 22, 2025 1:45 PM to 2:15 PM · 30 min. (Europe/Amsterdam)

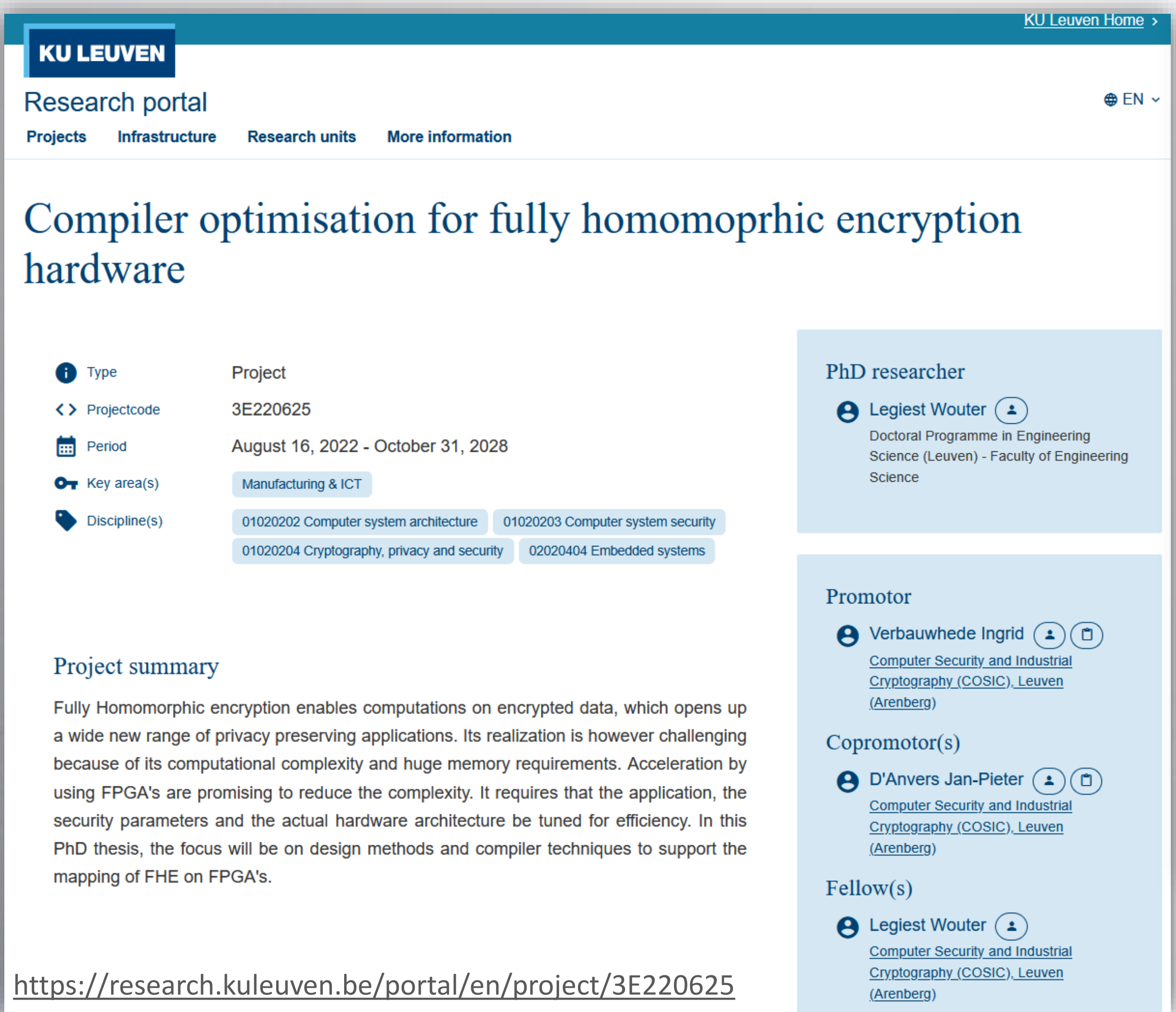
Tech Theater

Theater session

Speakers

JD **Jan-Pieter D'Anvers**
Employee
COSIC, KU Leuven

Fully Homorphic Encryption is (now) (will be) a thing



KU Leuven Home ›

KU LEUVEN

Research portal

EN ⌄

Projects Infrastructure Research units More information

Compiler optimisation for fully homomoprhic encryption hardware

Type	Project
Projectcode	3E220625
Period	August 16, 2022 - October 31, 2028
Key area(s)	Manufacturing & ICT
Discipline(s)	01020202 Computer system architecture 01020203 Computer system security 01020204 Cryptography, privacy and security 02020404 Embedded systems

Project summary

Fully Homomorphic encryption enables computations on encrypted data, which opens up a wide new range of privacy preserving applications. Its realization is however challenging because of its computational complexity and huge memory requirements. Acceleration by using FPGA's are promising to reduce the complexity. It requires that the application, the security parameters and the actual hardware architecture be tuned for efficiency. In this PhD thesis, the focus will be on design methods and compiler techniques to support the mapping of FHE on FPGA's.

PhD researcher

Legiest Wouter
Doctoral Programme in Engineering Science (Leuven) - Faculty of Engineering Science

Promotor

Verbauwhede Ingrid
Computer Security and Industrial Cryptography (COSIC), Leuven (Arenberg)

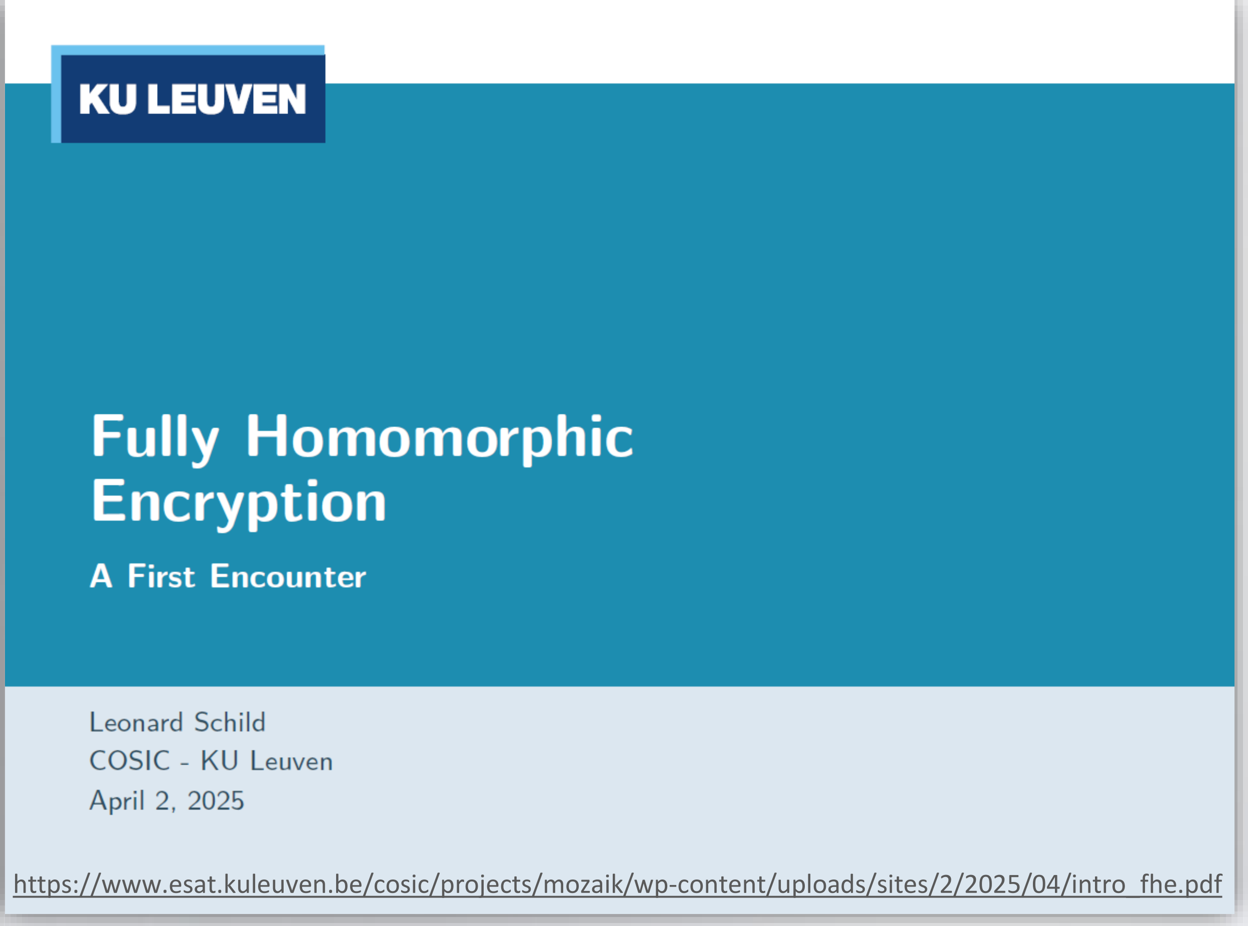
Copromotor(s)

D'Anvers Jan-Pieter
Computer Security and Industrial Cryptography (COSIC), Leuven (Arenberg)

Fellow(s)

Legiest Wouter
Computer Security and Industrial Cryptography (COSIC), Leuven (Arenberg)

https://research.kuleuven.be/portal/en/project/3E220625



KU LEUVEN

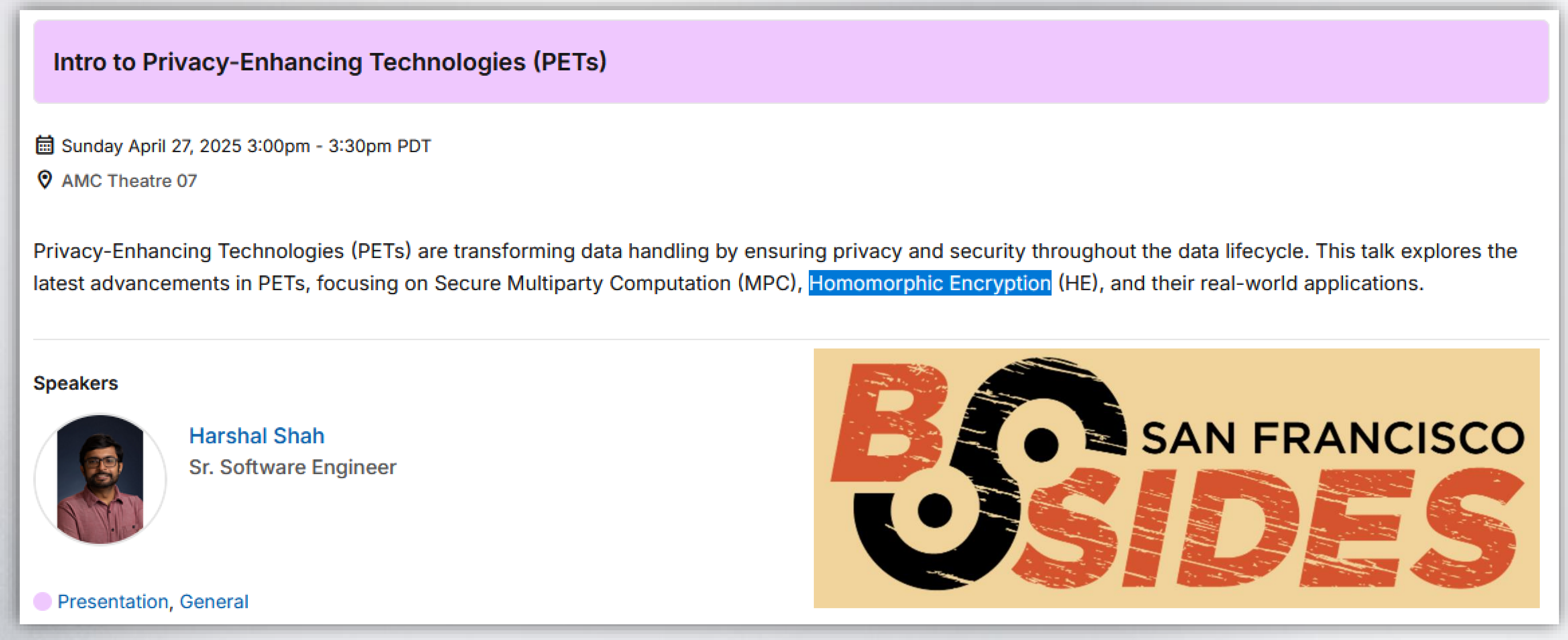
Fully Homomorphic Encryption

A First Encounter

Leonard Schild
COSIC - KU Leuven
April 2, 2025

https://www.esat.kuleuven.be/cosic/projects/mozaik/wp-content/uploads/sites/2/2025/04/intro_fhe.pdf

Fully Homorphic Encryption is (now) (will be) a thing



Intro to Privacy-Enhancing Technologies (PETs)

📅 Sunday April 27, 2025 3:00pm - 3:30pm PDT

📍 AMC Theatre 07

Privacy-Enhancing Technologies (PETs) are transforming data handling by ensuring privacy and security throughout the data lifecycle. This talk explores the latest advancements in PETs, focusing on Secure Multiparty Computation (MPC), Homomorphic Encryption (HE), and their real-world applications.

Speakers

Harshal Shah
Sr. Software Engineer

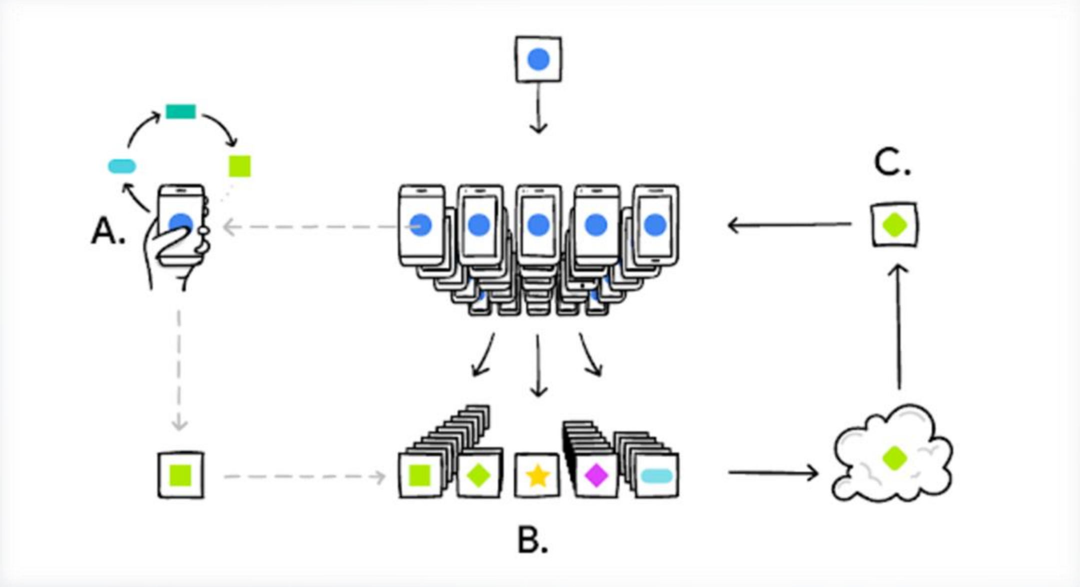
● Presentation, General

Federated Learning

- *Federated learning* is used to train a decentralized machine learning model amongst multiple participants

- It consist in collaboratively training a shared model while keeping the training data locally without exchanging it with a central location
  - It is not the data that is shared to build a model, but the *local* model is shared to build a *global* model

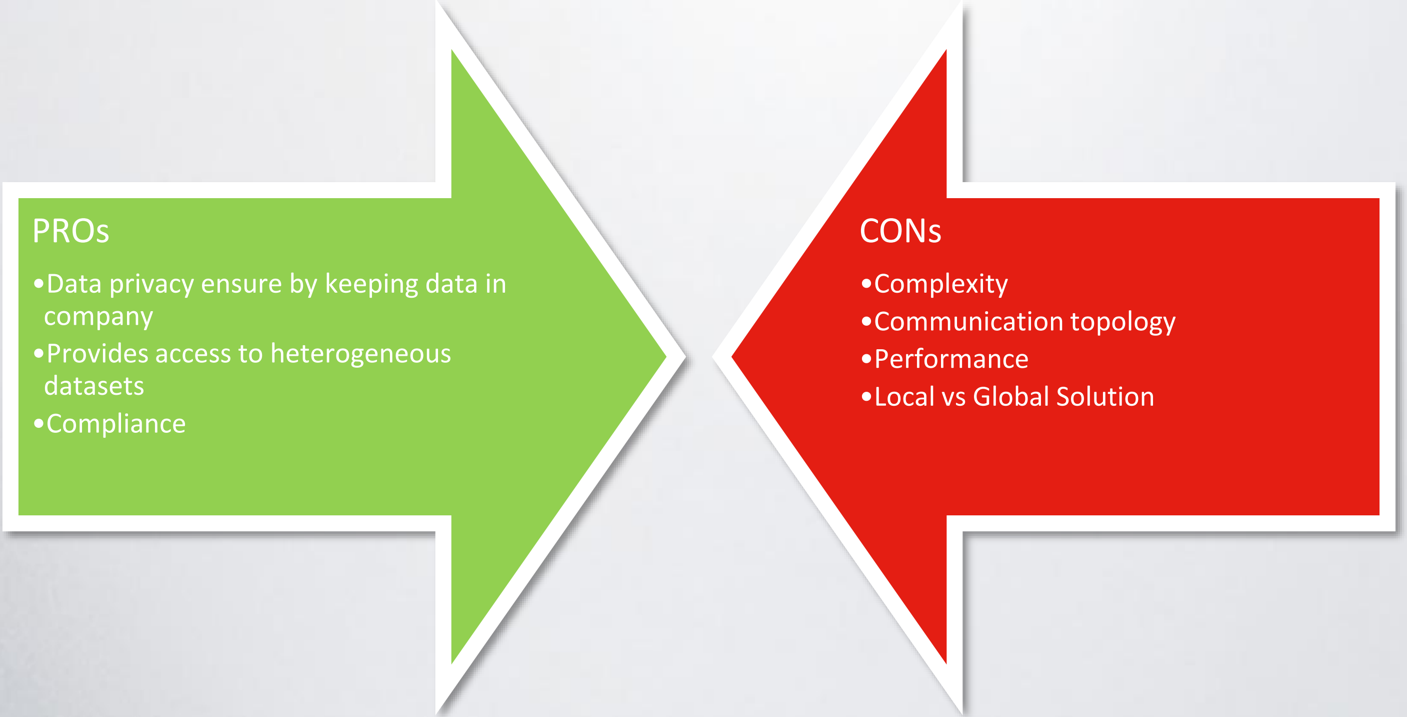
- The outcome of the federated learning model is a machine learning model that can be used by all participants for security model
  - The model is shared permanently during the learning phase
  - Outcome is a better trained model that has been fed with multiple and varied data



- The outcome of the federated learning model will be sharing over the open cyber security data space as an additional added value

- It creates an alternative to the traditional centralized approach to building machine learning models where data from different sources is collected and stored on one server

Federated Learning



PROs

- Data privacy ensure by keeping data in company
- Provides access to heterogeneous datasets
- Compliance

CONs

- Complexity
- Communication topology
- Performance
- Local vs Global Solution

- **Use-cases**
  - Mobile Apps
    - Google uses federated learning to improve on-device machine learning for their Google Assistant (voice commands)
  - Financial Services
    - Allows sharing of AML/KYC models across banks
  - Healthcare
    - Protects sensitive data and can provide data diversity to diagnose rare diseases
  - Autonomous Vehicles
    - Provide better and safer self-driving car experience with real-time data and predictions from fleet of cars

Combining *Federated Learning* & *Homomorphic Encryption*

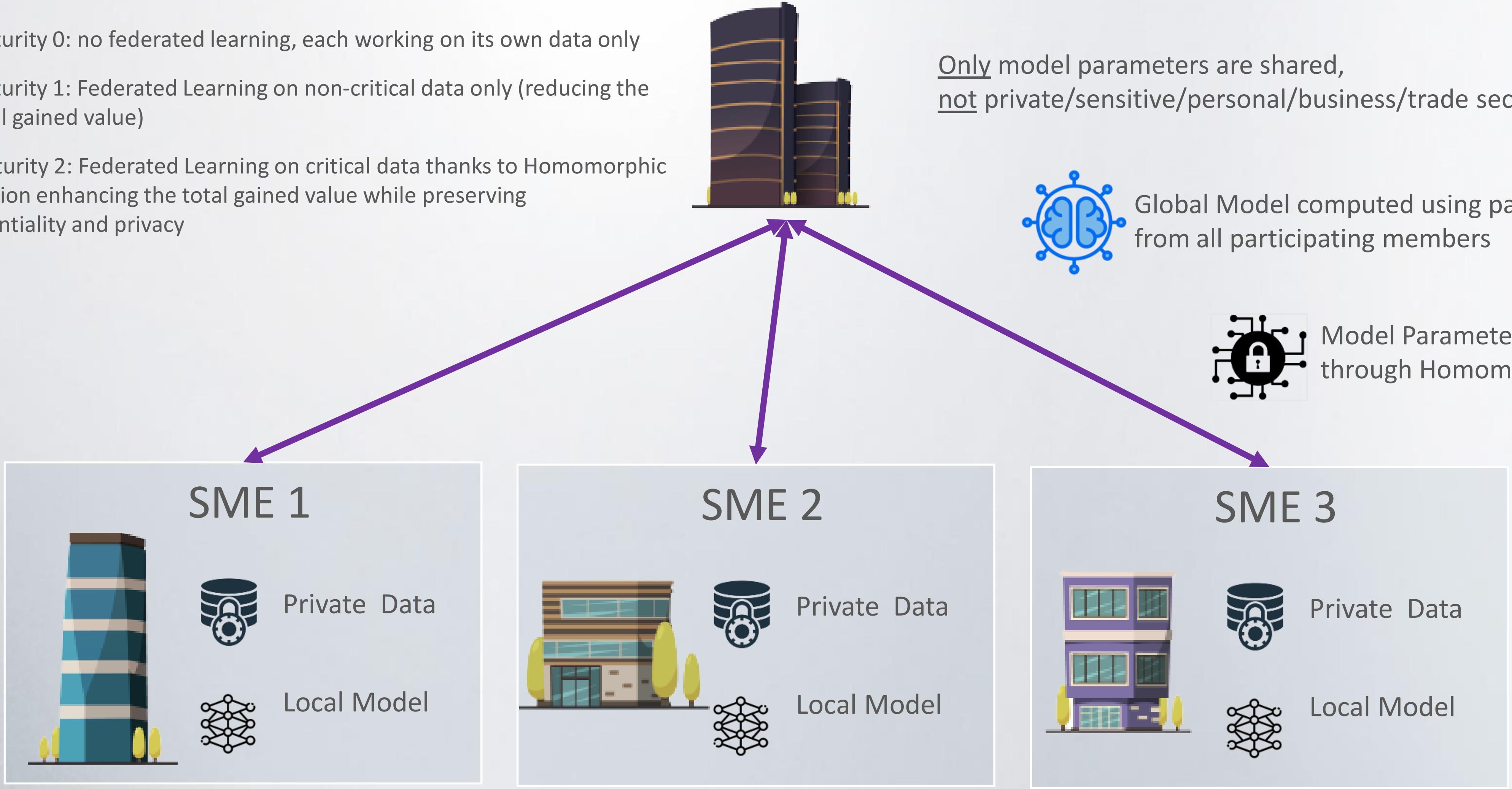
- Maturity 0: no federated learning, each working on its own data only
- Maturity 1: Federated Learning on non-critical data only (reducing the total gained value)

→ Maturity 2: Federated Learning on critical data thanks to Homomorphic Encryption enhancing the total gained value while preserving confidentiality and privacy

Only model parameters are shared,
not private/sensitive/personal/business/trade secrets/IPR

Global Model computed using parameters from all participating members

Model Parameters secured through Homomorphic Encryption



SME 1

Private Data

Local Model

SME 2

Private Data

Local Model

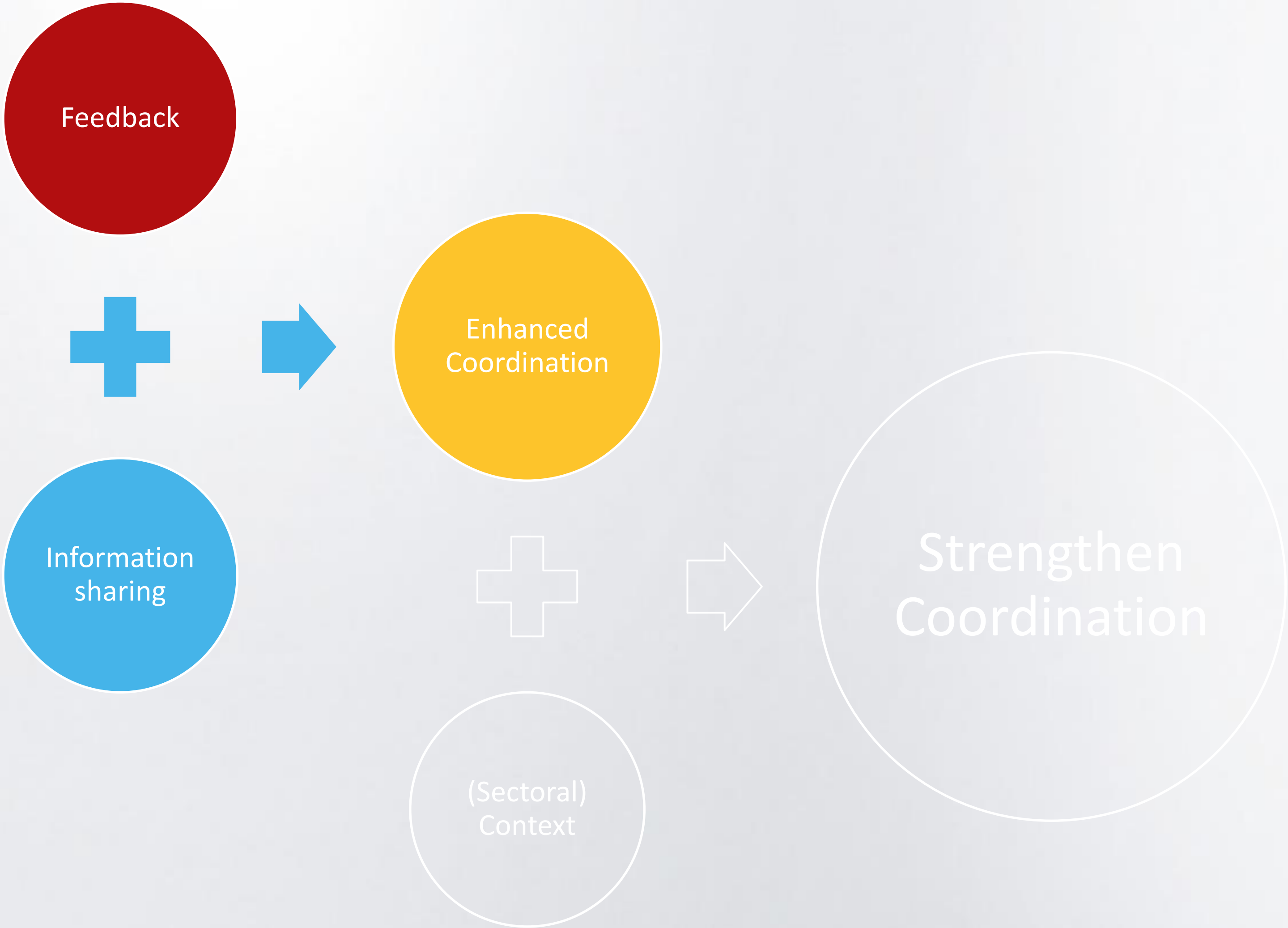
SME 3

Private Data

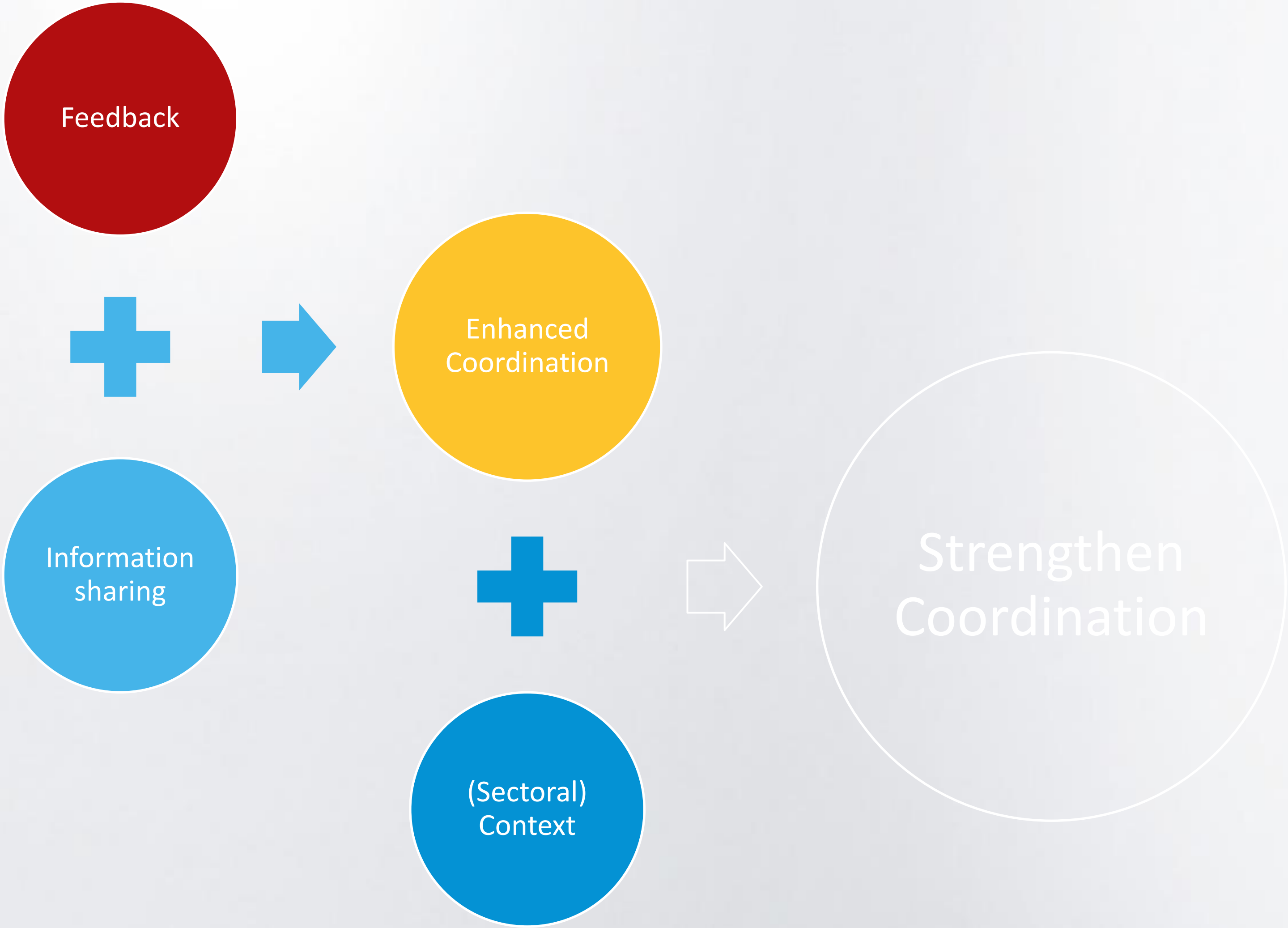
Local Model

Uplink: local model parameters
Downlink: global model

How to *enhance* coordination?

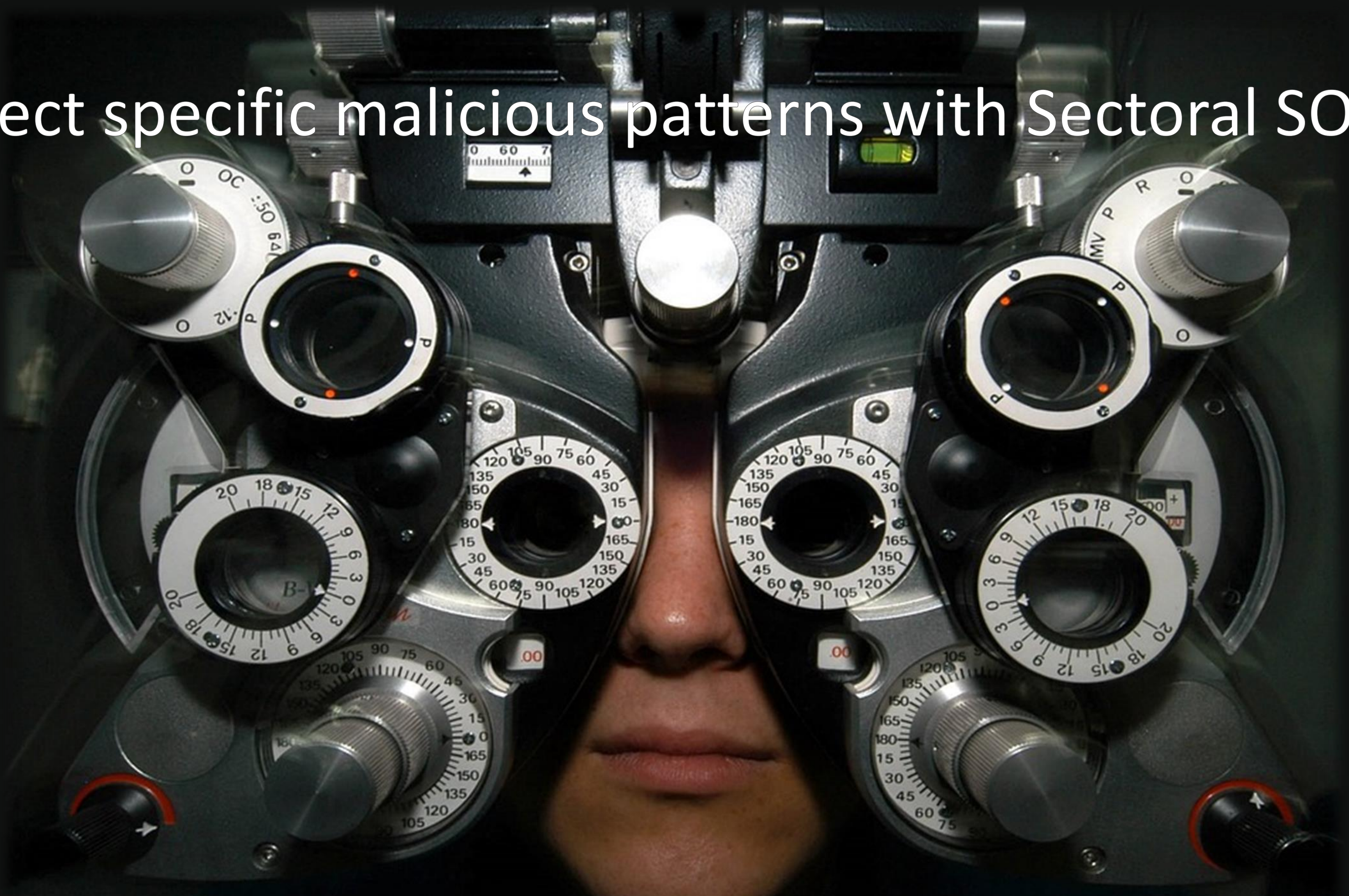


How to *strengthen* coordination?

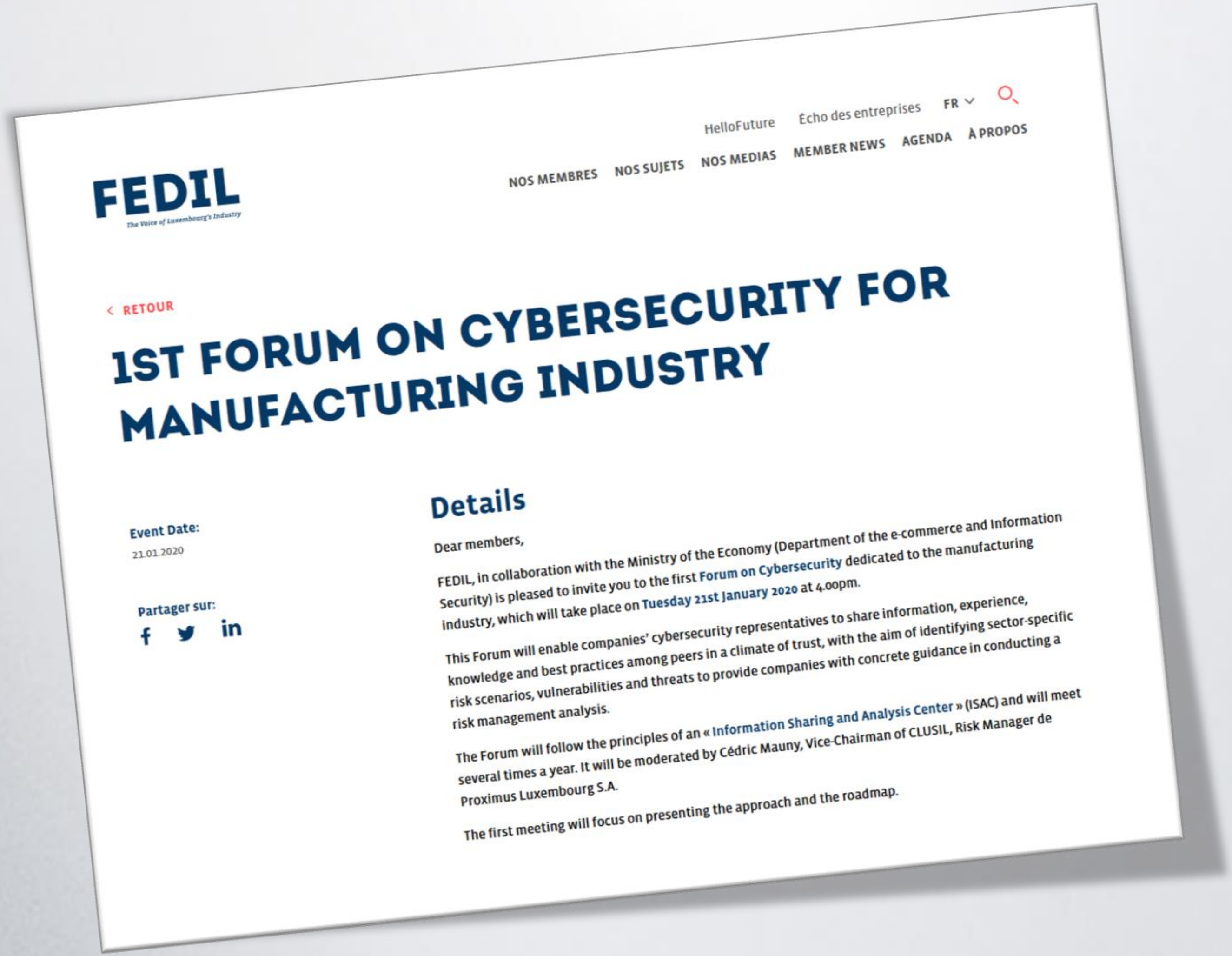


Think *sectoral risks*

Detect specific malicious patterns with Sectoral SOC



Setup a (sectoral) *Trusted Network* and share the knowledge within the (sectoral) *Trusted Network*



1ST FORUM ON CYBERSECURITY FOR MANUFACTURING INDUSTRY

Event Date:
21.01.2020

Partager sur:

Details

Dear members,

FEDIL, in collaboration with the Ministry of the Economy (Department of the e-commerce and Information Security) is pleased to invite you to the first Forum on Cybersecurity dedicated to the manufacturing industry, which will take place on Tuesday 21st January 2020 at 4.00pm.

This Forum will enable companies' cybersecurity representatives to share information, experience, knowledge and best practices among peers in a climate of trust, with the aim of identifying sector-specific risk scenarios, vulnerabilities and threats to provide companies with concrete guidance in conducting a risk management analysis.

The Forum will follow the principles of an « Information Sharing and Analysis Center » (ISAC) and will meet several times a year. It will be moderated by Cédric Mauny, Vice-Chairman of CLUSIL, Risk Manager de Proximus Luxembourg S.A.

The first meeting will focus on presenting the approach and the roadmap.

- Implementation of NIS2 in Luxembourg intents to rely on ISAC for the different economic sectors to valorize the approach of Informed Governance while ensuring a better management of risks from a sectoral perspective

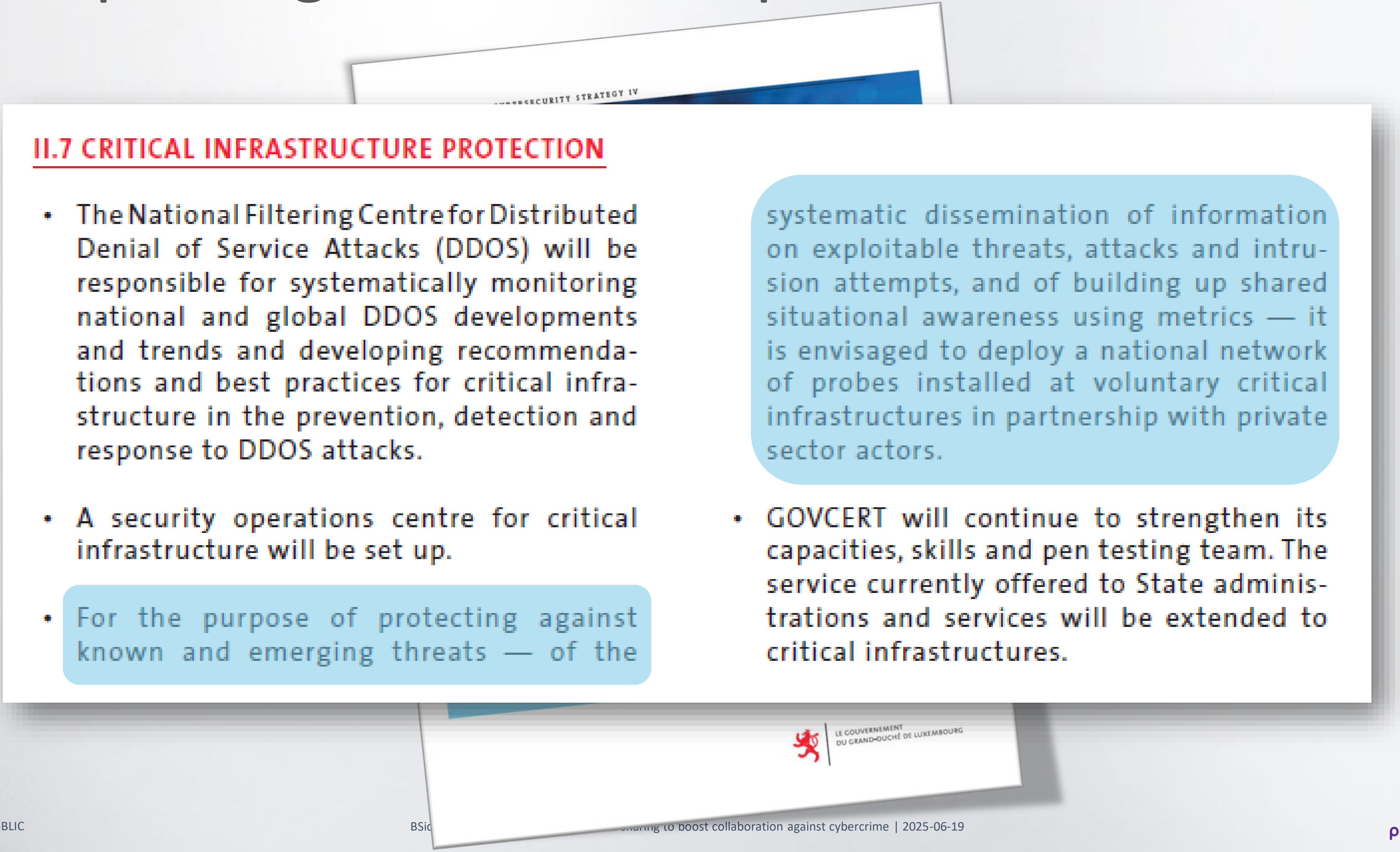
Coordination against cybercrime…

NATIONAL CYBERSECURITY STRATEGY IV

NATIONAL CYBERSECURITY STRATEGY IV

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

… by improving detections capabilities within sectors



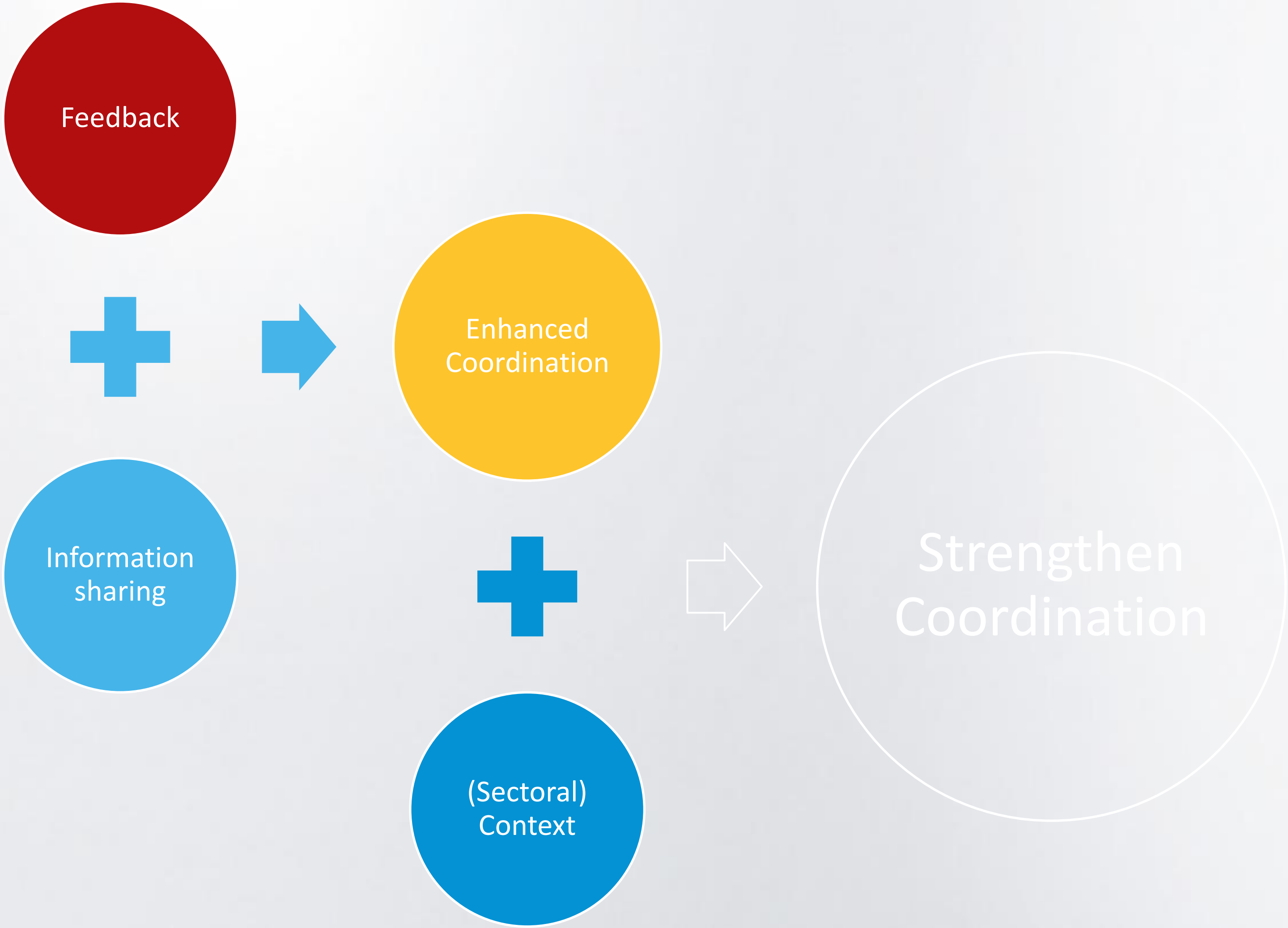
CYBERSECURITY STRATEGY IV

II.7 CRITICAL INFRASTRUCTURE PROTECTION

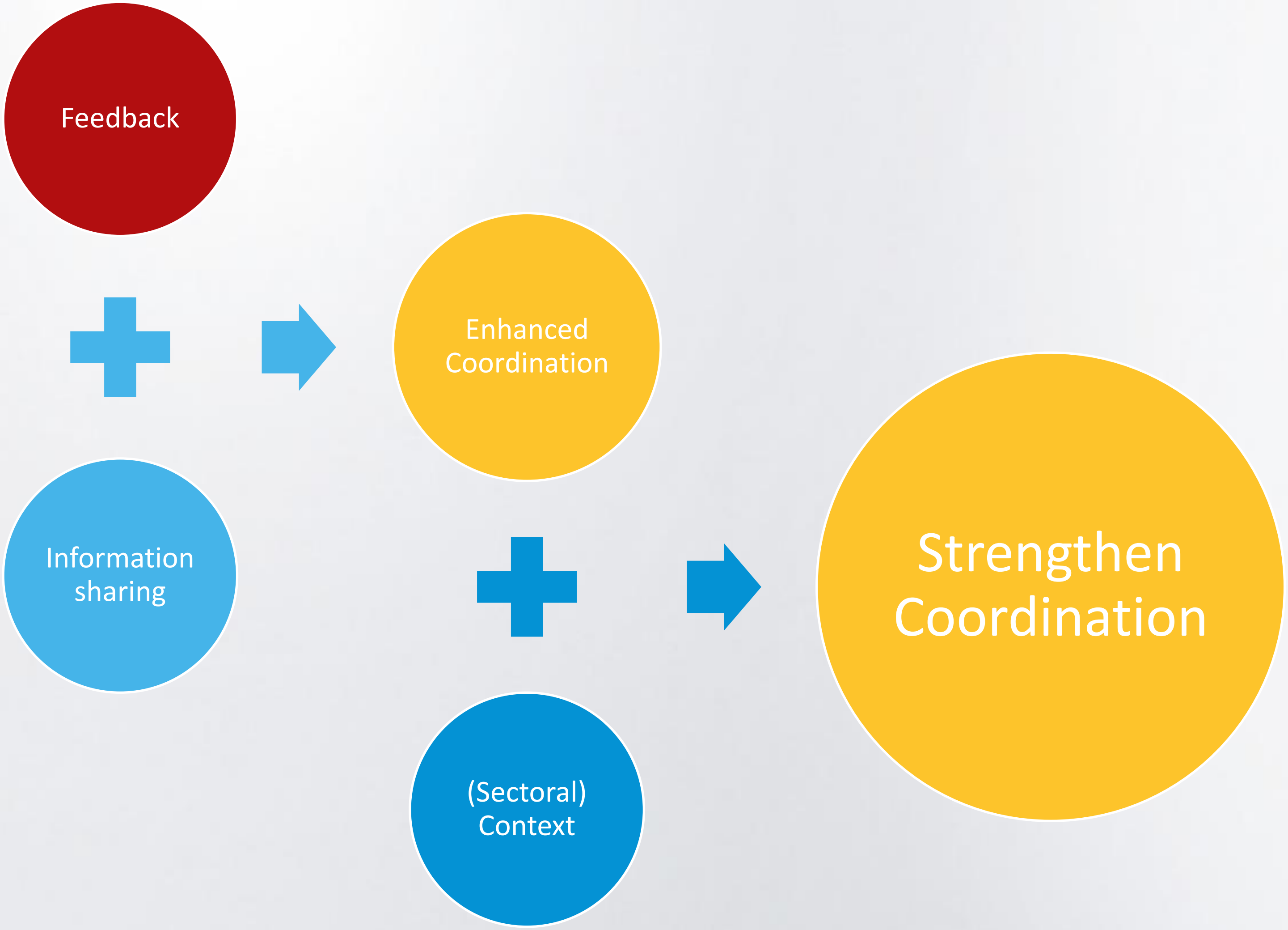
- The National Filtering Centre for Distributed Denial of Service Attacks (DDOS) will be responsible for systematically monitoring national and global DDOS developments and trends and developing recommendations and best practices for critical infrastructure in the prevention, detection and response to DDOS attacks.
- A security operations centre for critical infrastructure will be set up.
- For the purpose of protecting against known and emerging threats — of the systematic dissemination of information on exploitable threats, attacks and intrusion attempts, and of building up shared situational awareness using metrics — it is envisaged to deploy a national network of probes installed at voluntary critical infrastructures in partnership with private sector actors.
- GOVCERT will continue to strengthen its capacities, skills and pen testing team. The service currently offered to State administrations and services will be extended to critical infrastructures.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

How to *strengthen* coordination?



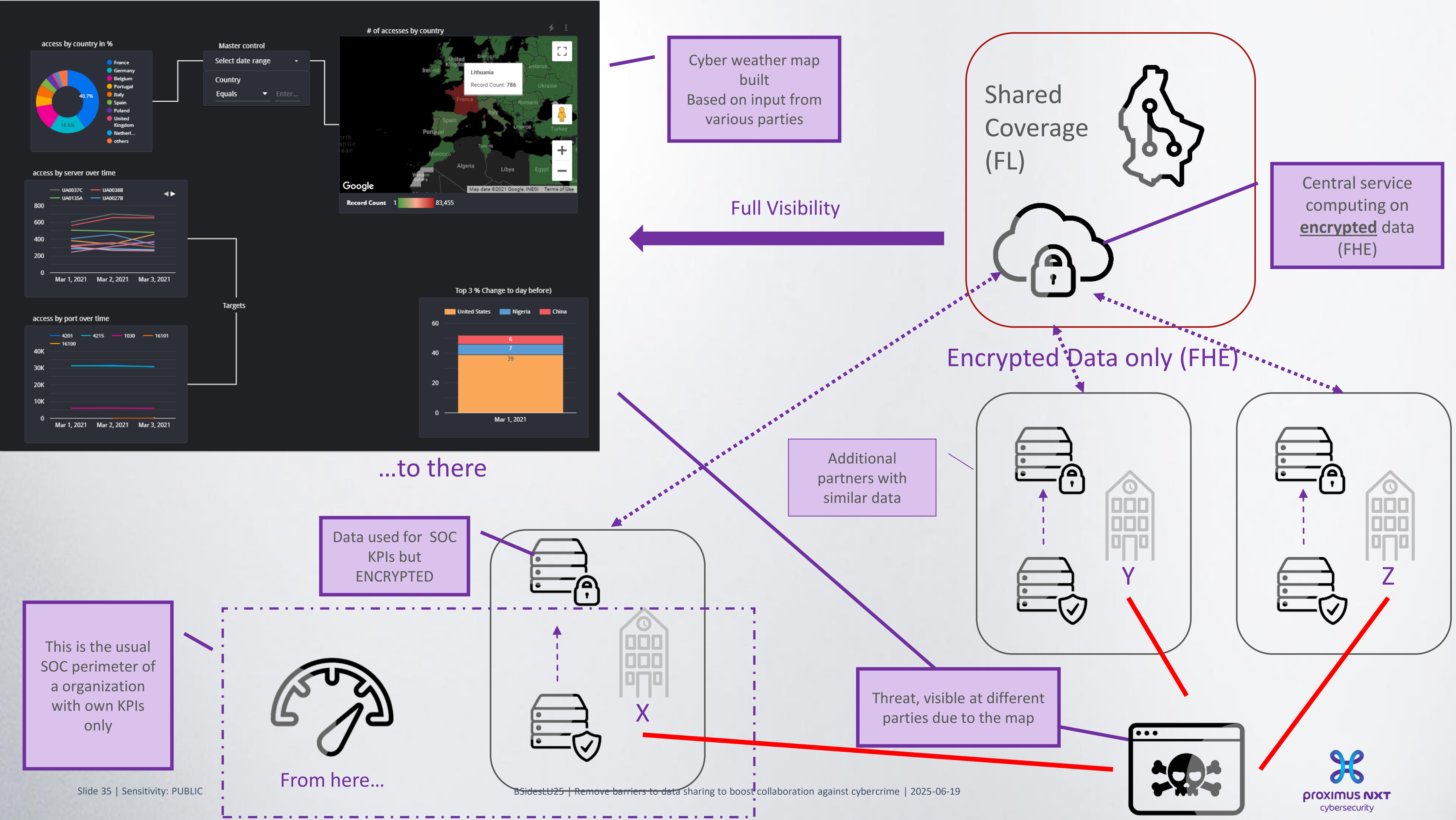
How to *strengthen* coordination?



You are not alone / We are not alone

Sharing is caring

We are all interconnected



Cyber weather map built
Based on input from various parties

Shared Coverage (FL)

Central service computing on **encrypted** data (FHE)

Full Visibility

Encrypted Data only (FHE)

…to there

Additional partners with similar data

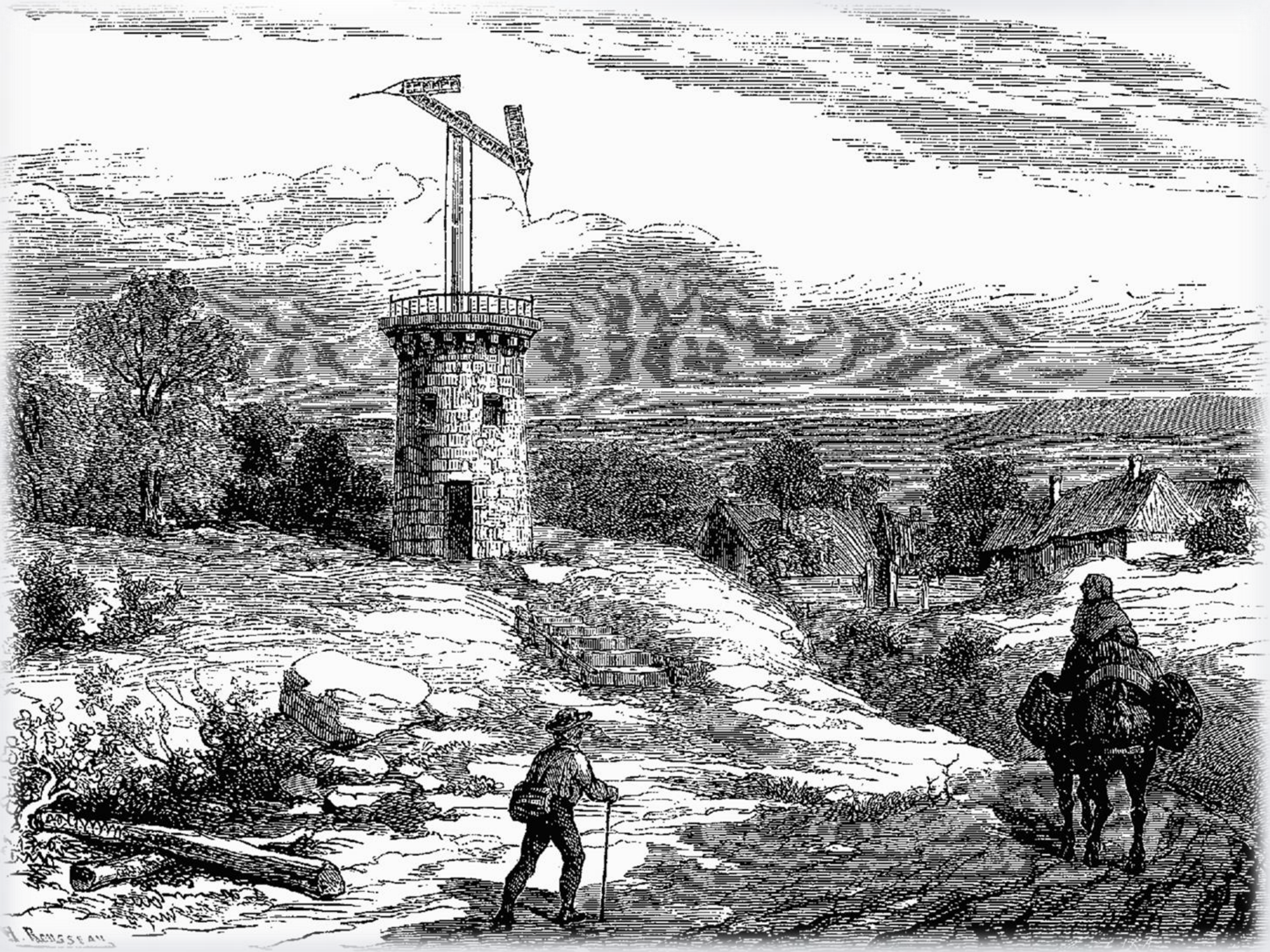
Data used for SOC KPIs but ENCRYPTED

This is the usual SOC perimeter of a organization with own KPIs only

From here…

Threat, visible at different parties due to the map

Share the knowledge within the (sectoral) *Trusted Network*



Thank you

for your attention

●●● www.proximusnxt.lu

Questions

& Answers

●●● www.proximusnxt.lu

Contact Information

Cédric MAUNY

cedric.mauny@proximus.lu

(+352) 621.200.707

in https://www.linkedin.com/in/cedricmauny/

proximus NXT

cybersecurity