ECCO
European Cybersecurity COmmunity

Digital Europe Programme Cybersecurity

Pitch ideas

Chaired by Roberto Cascella

ECCO Project Coordinator

ECCC Infoday Milan – 7th November 2024

This deliverable was prepared for DG CNECT by the ECCO Consortium under contract° CNECT/2022/OP/0033 and is the European Commission's property. The views expressed in this document are purely those of the authors and may not, in any circumstances, be interpreted as stating an official position of the European Commission. The European Commission does not guarantee the accuracy of the information included in this document, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the authors to ensure that they have obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 - Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

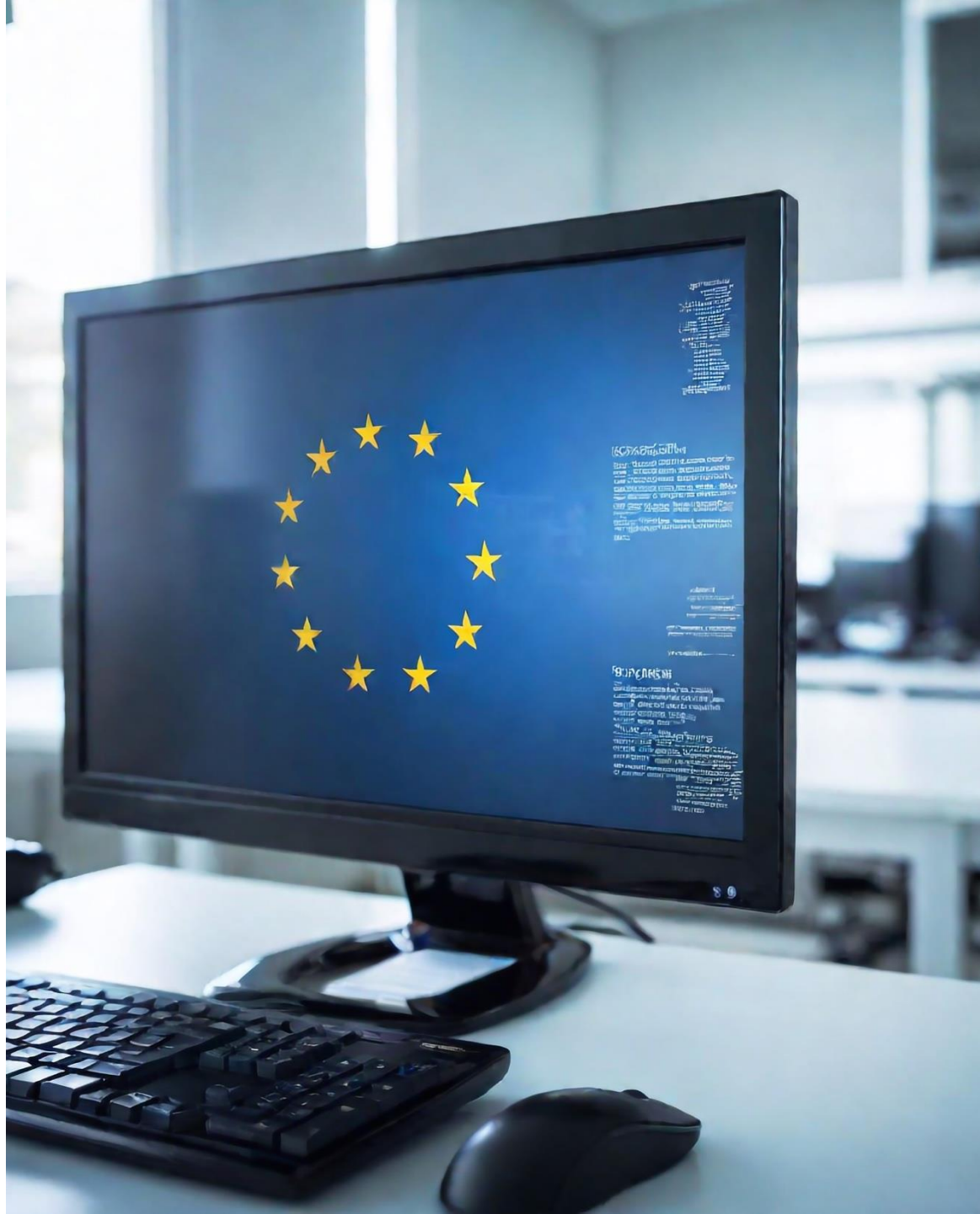
#	ORGANISATION	PRESENTER
1	Vulnir	Angelo D'Amato

Vulnir

CREA

Cyber Resilience Enhanced Assessment

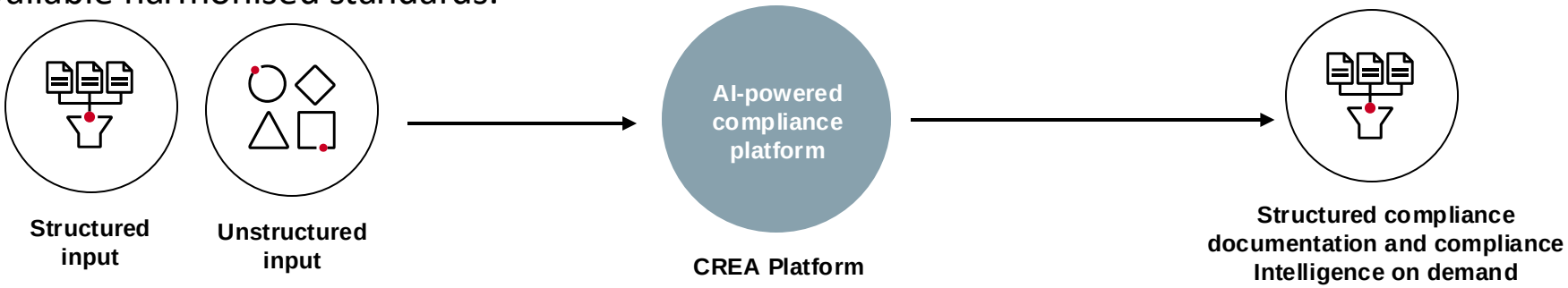
Angelo D'Amato
Cybersecurity and Compliance Expert



DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02 Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

Challenges for stakeholders

- Lack of **cybersecurity skills** to cover the upcoming demand for manufacturers and for notified bodies/Conformity Assessment Bodies (CAB). (e.g. introducing **more automation** can mitigate this problem)
- Need to reduce the impact of **cybersecurity standards landscape fragmentation** with a more integrated approach (e.g., ETSI EN 303 645 vs EN 18031)
- Need to manage the complexity and **interplay of the cybersecurity conformity assessment** for the organization and product lifecycle and **identify the gaps** (e.g., Bridge the gaps between organizational policies and product implementation) **proactively**
- Need to reduce the time to market and provide a **continuous compliance monitoring** mechanisms that **seamlessly integrate with the organization information sources** enabling the required automation and workflows (e.g. Reporting obligations) as required by the new upcoming cybersecurity regulations (e.g. CRA)
- **Learn from the past and centralize the knowledge** in a single platform (e.g., from a recurrent technical and non-technical issues)
- **Need to share the knowledge** with a possibility to generate and extract synthetic data to stimulate knowledge sharing about product security testing plans, threats, incidents and common issues with market surveillance or with Cooperation Group and the CSIRTs Network to enable the creation of market benchmarks and contribute to improve available harmonised standards.



Desired Outcomes

SMEs / Manufacturers: **AI-powered platform** whose aim is **to automate internal compliance procedures**, including testing and specification drafting, which can ease the burden on SMEs, improving efficiency and enable guided and centralized approach **to prepare for future compliance with RED, CRA, CSA, NIS2**. In addition, the platform will allow for integrated **monitoring of the entire product security lifecycle** and increase the speed of **the incident response team's triage and reporting** activities. The platform should be able to **export synthetic data** in a way to enable knowledge sharing about product and organizations security properties with market surveillances network keeping in consideration privacy concerns.

Market Surveillance / Notified bodies / Manufacturers: CREA platform **streamlines conformity assessment exchanges**, making it easier for authorities to obtain information from manufacturers in a structured, **machine-readable format**.
Notified bodies can leverage our platform to compare assessments, correlate data for similar products, and **refine test plans and testing methodologies** for similar category of products creating more **standardizing approach towards the derivation of a testing report**. The retrieval-augmented generation (RAG) model will allow the platform to **”learn from the past”** enhancing its efficiency and accuracy in identifying risks and to derive more accurate threat-based testing scenarios.

Looking for partners

Manufacturer / SME

To offer collaboration for the integrations and development of the first version of the platform with relevant training data set for the AI Model and explore synthetic data efficiency.

Platform Development

Platform development company that will help in creating a scalable software and infrastructure architecture and for product productization.

AI Research partner

Prototyping and productizing an innovative AI core module that is trained for cybersecurity evaluations and aligned with the available cybersecurity standards and conformity assessment procedures.

Targeted objectives

Objectives:

- Supporting market surveillance authorities/notifying authorities/national accreditation bodies to implement the CRA.
- Support cybersecurity certification in line with the amended Cybersecurity Act.

Priorities:

- Increasing capacity for market surveillance authorities/notifying authorities/national accreditation bodies in view of tasks as provided by the CRA.
- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.

Outcomes:

- Support actions and cooperation for further advanced of cybersecurity certification.

Let’s Work Together

VULNIR | Securing your digital success

CONTACT:

Angelo D’Amato
Cybersecurity and Compliance Expert

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

info@vulnir.com

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies

#	ORGANISATION	PRESENTER
1	Cyberecocul Global Services	Marios Thoma
2	Equixly	Mattia Fedrizzi

CyberEcoCul

Early identification of Advance Persistent Threats (APTs)

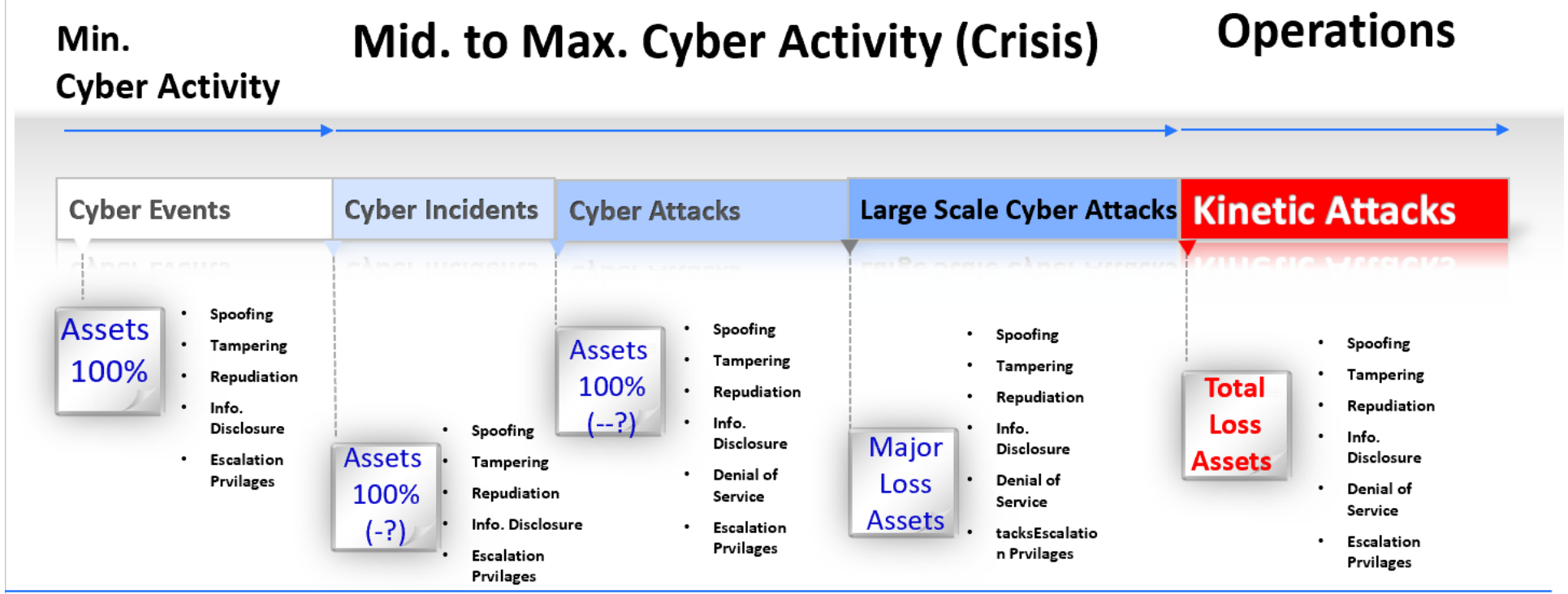
Focus : DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH - Development and Deployment of Advanced Key Technologies

Dr. Marios THOMA
Cyber Expert – Researcher APTs
Email : marios.thoma@cytanet.com.cy
Cyberecocul Global Services : www.cyberecocul.com

Milano, 07 November 2024

CyberEcoCul

Early identification of Advance Persistent Threats (APTs)



Background : Already a lot of research on the Detection of Information Collaborative Misbehavior in Cyber Attacks (example)

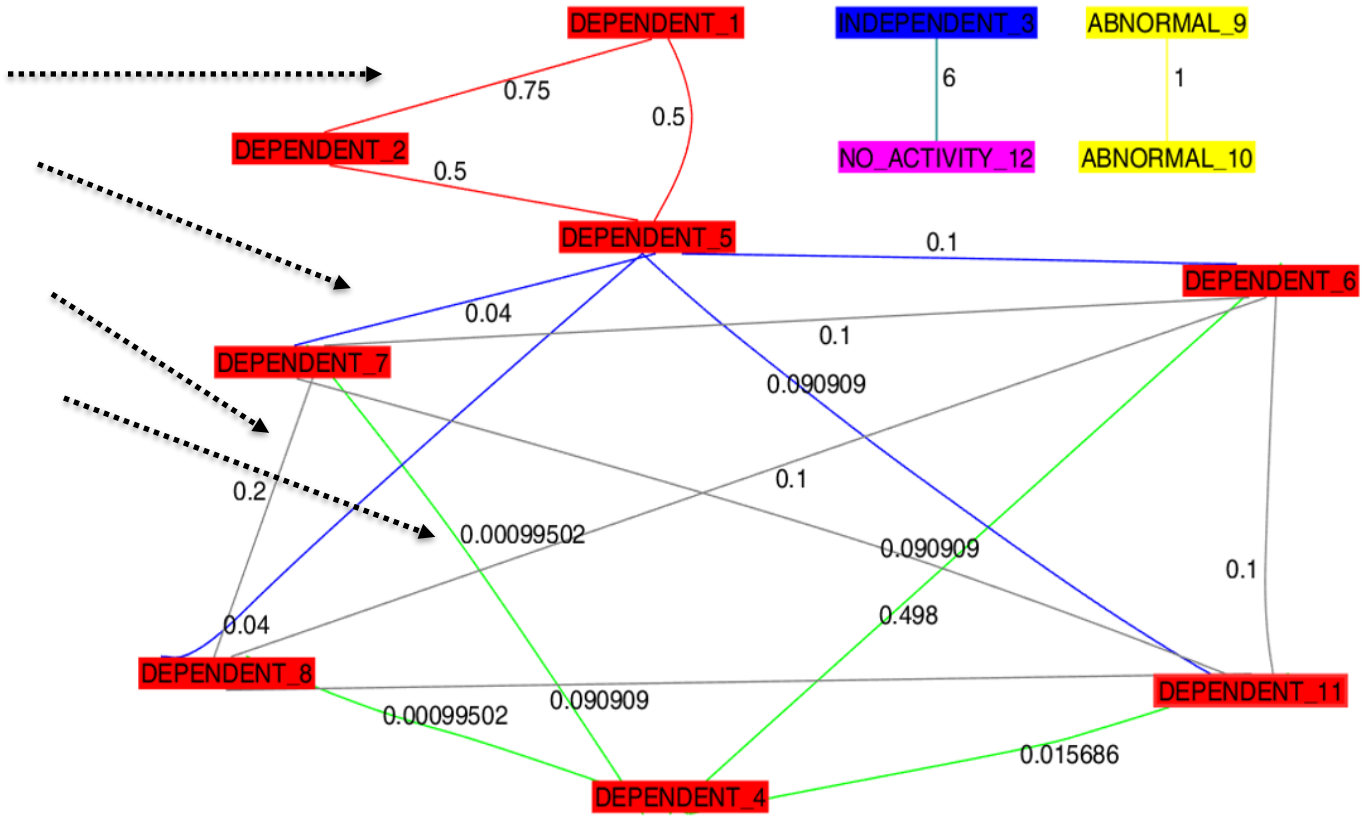
Dependent Users

1st Clique - RED EDGES

2nd Clique - BLUE EDGES

3rd Clique - GREY EDGES

4th Clique - GREEN EDGES

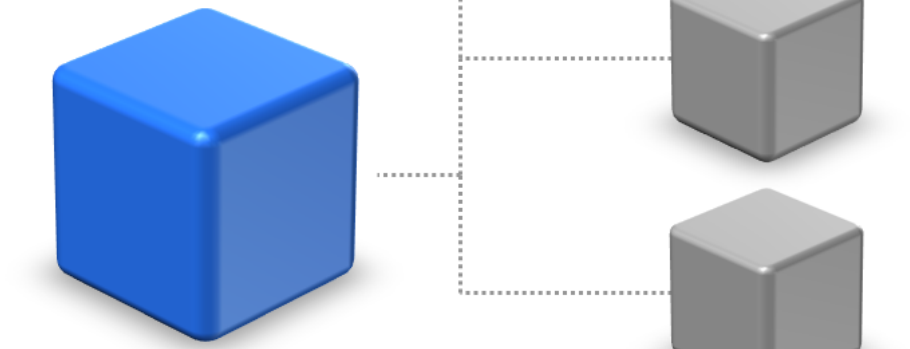


Artificial Intelligence (AI) :

Improve the pattern recognition and the early identification of Distribution Denial of Service (DDoS) Attacks.

CyberEcoCul

Early identification of Advance Persistent Threats (APTs)



Description
of the proposal

Status
- On going

Capabilities
- Operational
- Technical / R & D

Type of partners
- Private Operational entities
- Research and Academia
- Governmental Operational entities

The AI-Powered Hacker to Secure your API

Call: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH – Development and Deployment of Advanced Key Technologies

THE NEXT-GEN API SECURITY TESTING PLATFORM, NOW

equixly

API PROTECTION PROBLEM

83% of internet traffic is APIs

$5M+ cost of an average data breach

10x more leaked data in API breaches than average security breaches

Weeks needed for professionals to complete penetration testing

10% vulnerabilities spotted via today’s solutions

Source: Gartner (2024), Akamai (2024)

equixly

THE EQUIXLY SOLUTION

SECURITY POSTURE

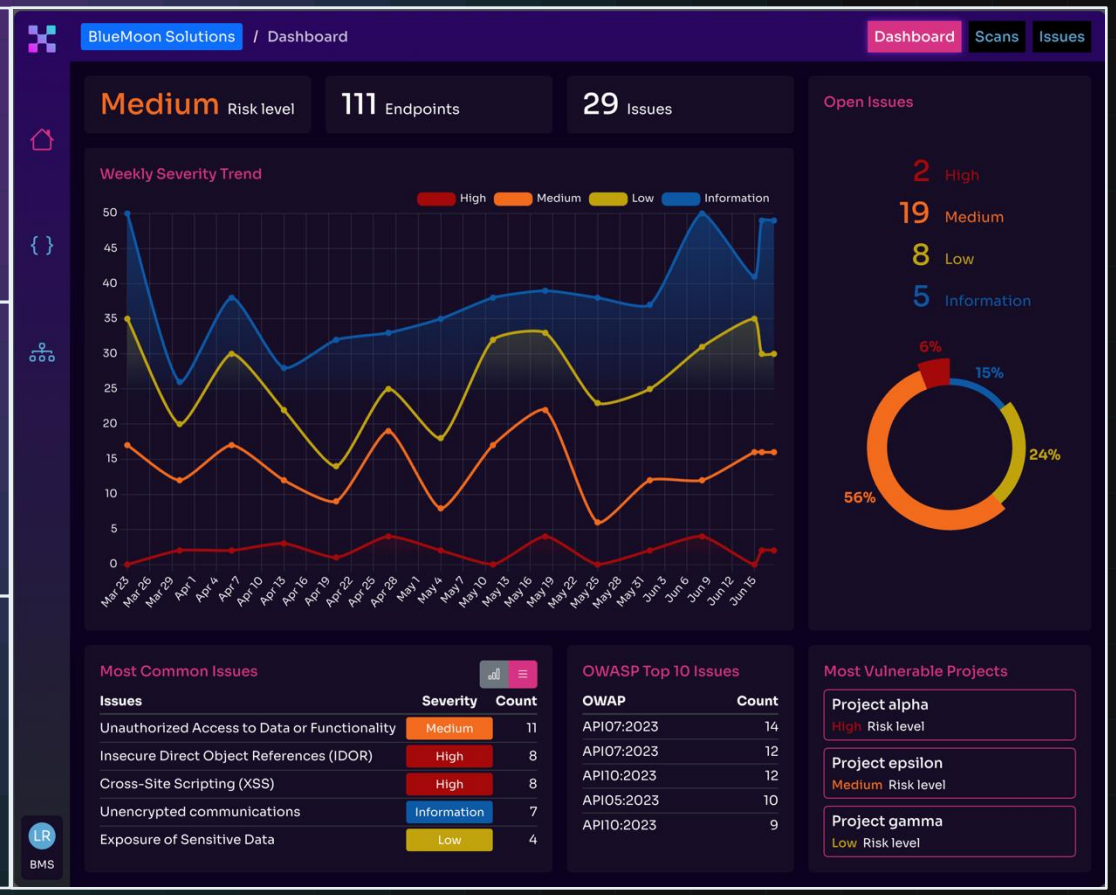
- API INVENTORY
- DATA CLASSIFICATION

PROACTIVE TESTING

- SCALABLE AND CONTINUOUS
- DEV PIPELINE INTEGRATION

SIMPLIFIED COMPLIANCE

- SECURITY RISKS
- REPORTING



AI-POWERED PLATFORM

PERFORMANCE AT A GLANCE

Human	Equixly
154 HOURS (20 DAYS)	**4-6 HOURS**
40% of perimeter tested	100% of perimeter tested
2 FTEs	0 FTEs
One off	Continuous

Source: Equixly analysis based on an application of 40 endpoints and 210 sequences/endpoint (2024)

THANK YOU

MEET US

Equixly – Head Office

Via E. Torricelli, 8A

37135 Verona (VR), Italy

WRITE US

Follow up questions

mattia.fedrizzi@equixly.com

Sales Team

sales@equixly.com

VISIT US

Website

https://equixly.com/

Blog

https://equixly.com/blog/

Linkedin

BOOK A CALL

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

#	ORGANISATION	PRESENTER
1	Cyberecocul Global Services	Marios Thoma
2	Latvijas Mobilais Telefons SIA	Mārtiņš Kaļķis and Evija Plone

Post – Quantum Cryptography in the context of CI interconnections

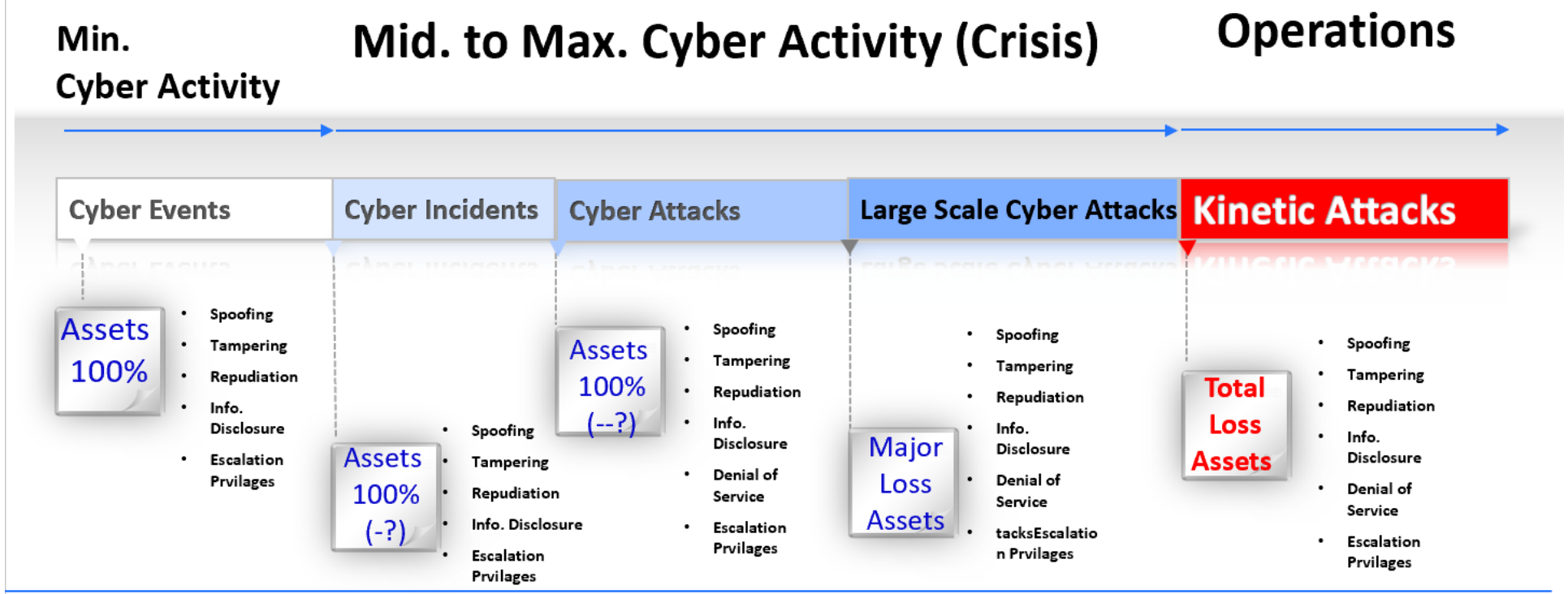
Focus : DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER - Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

Dr. Marios THOMA
Cyber Expert – Researcher APTs
Email : marios.thoma@cytanet.com.cy
Cyberecocul Global Services : www.cyberecocul.com

Milano, 07 November 2024

CyberEcoCul

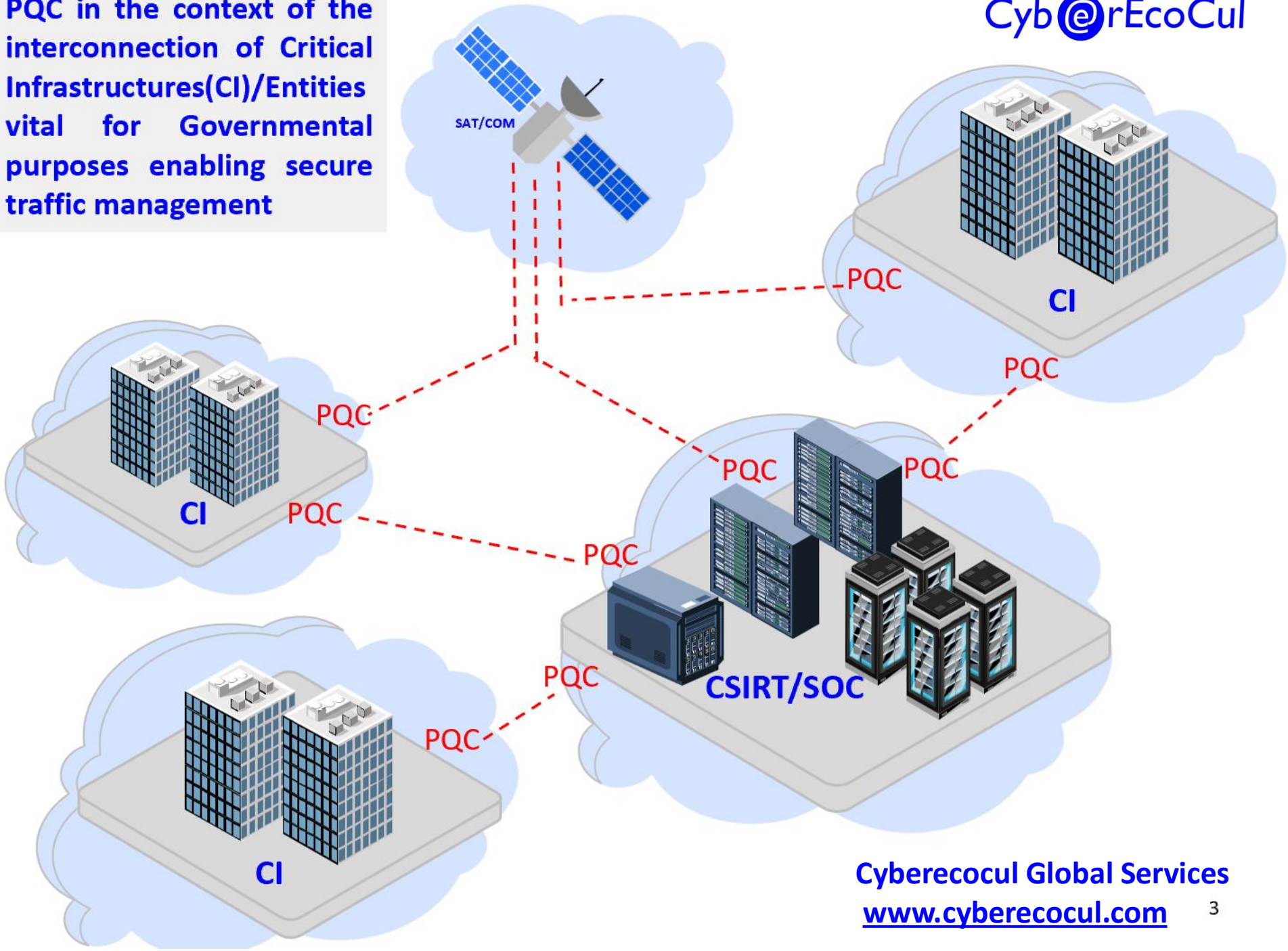
Post – Quantum Cryptography in the context of CI interconnections



Cyberecocul Global Services
www.cyberecocul.com

PQC in the context of the interconnection of Critical Infrastructures(CI)/Entities vital for Governmental purposes enabling secure traffic management

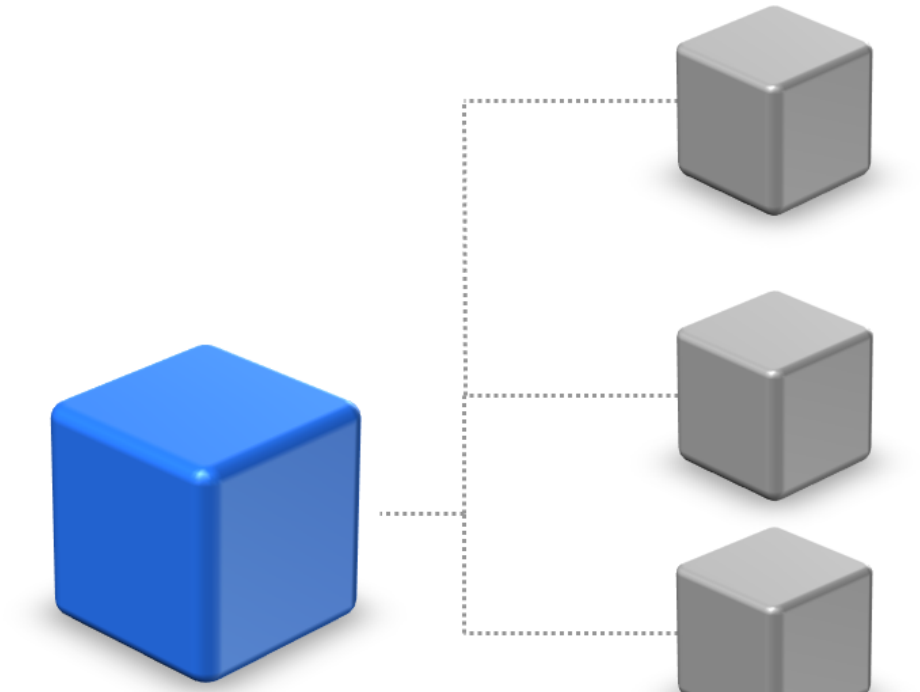
CyberEcoCul



Cyberecocul Global Services
www.cyberecocul.com

CyberEcoCul

Post – Quantum Cryptography in the context of CI interconnections



Description
of the proposal

Status
- UCY
- Backbone
- Cyberecocul Global Services

Capabilities
- Operational
- Technical / R & D

Type of partners
- Private Operational entities
- Research and Academia
- Governmental Operational entities

Critical Infrastructure eXchange for Preparedeness Support Services (CIX-PSS)

CALL: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER

Mārtiņš Kaļķis
Head of Cyber Security Division
Latvijas Mobilais Telefons, SIA

ECCC Info Day on the Digital Europe Programme
Funding Opportunities | 7 November 2024, Milan, Italy

LMT experience & partners in EU and R&D projects

Actual:

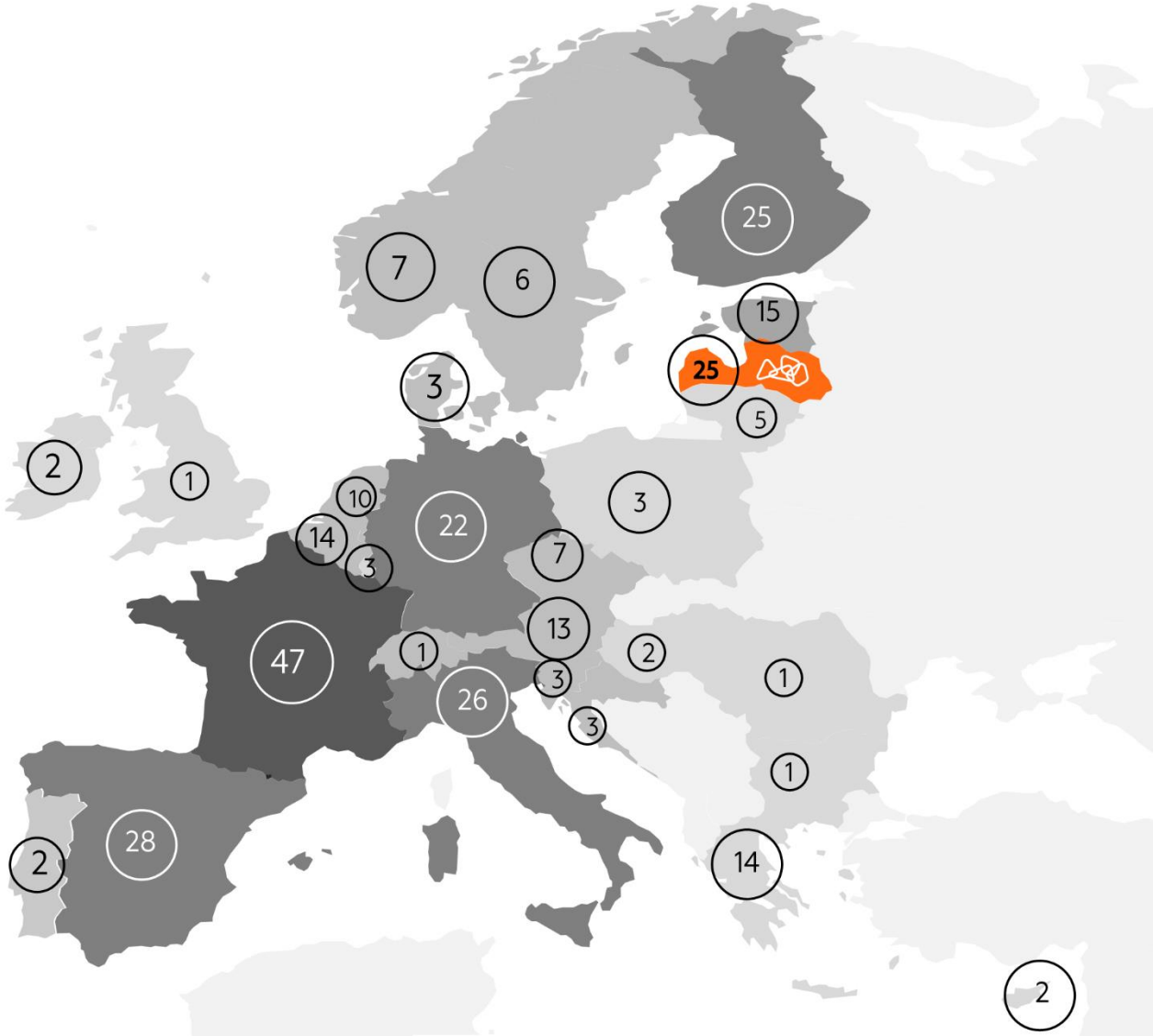
8 projects

290 partners

27 countries

Finalized:

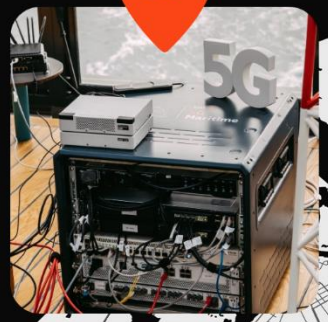
6 projects



LMT test sites

5G at Sea

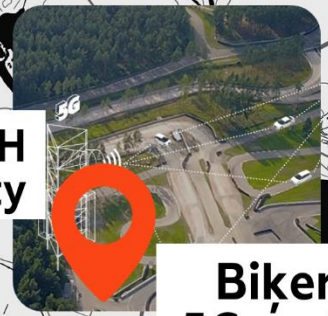
LVR FLOTE



Ādaži
5G Defence

Kīšezers Lake
Drone corridor

5G EMC Lab



VEFRESH
Smart City

Biķernieki
5G mobility

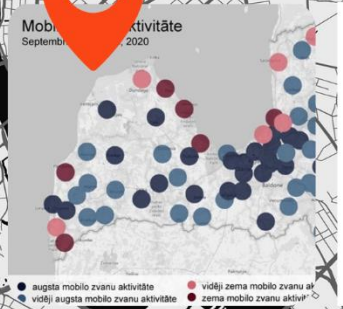
333
Drone testbed

RĪGA STRADIŅŠ UNIVERSITY

Health tech

1862
RIGA TECHNICAL UNIVERSITY

IoT, AI, 5G/6G



UNIVERSITAS LATVIENSIS SCIENTIAE ET PATRIAE
UNIVERSITY OF LATVIA

Quantum technologies, big data

The problem:

1. Ever rising threat level
   (according to LV-CERT and our own statistics)
2. NIS2 produces specific cyber challenges and brings emphasis on testing

Testing Critical Infrastructure requires technical expertise and a way to exchange this knowledge

For Cyberrange to be successful, it needs **quality content that is constantly updated** and relevant to specific industry

The solution:

CyberAttack and CyberDefence scenario Content Development and Exchange Platform for Critical Infrastructure Operators

- Building Platform
- Defining Common Language
- Creation of Red Team, Blue team and Training Scenarios
- Development of business model and platform
- Explore AI Based Threat Assessment

LMT and potential partnership

LMT advantages:

Experience in **EU** and **NATO R&D** projects

Multiple Internal **5G test labs**

Experience in being a **telecom**, **critical infrastructure**, **cybersecurity** provider

Looking for representatives of main types of critical infrastructure **with cyber security expertise:**

- Energy
- Health
- Transport
- Finance
- Public administration
- Space
- Water supply
- Digital infrastructure

** NIS2 context*

lmt

THINK - DO

Mārtiņš Kaļķis
Head of Cyber Security Division
Martins.Kalkis@lmt.lv
+371 29 248 605

Evija Plone
Innovation Project Lead
Evija.Plone@lmt.lv
+371 29 248 401

innovations.lmt.lv

ECCO
European Cybersecurity COmmunity

Thank you

European Commission

ECCO (European Cybersecurity COmmunity) has received funding under a contract with the Union. The content of this presentation does no
represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.