ECCO

European Cybersecurity COmmunity

Digital Europe Programme Cybersecurity

Pitch ideas

Chaired by Roberto Cascella

ECCO Project Coordinator

ECCC Infoday Bucharest – 22nd February 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-06-ENABLINGTECH
Novel applications of AI and Other Enabling Technologies for Security Operation Centres

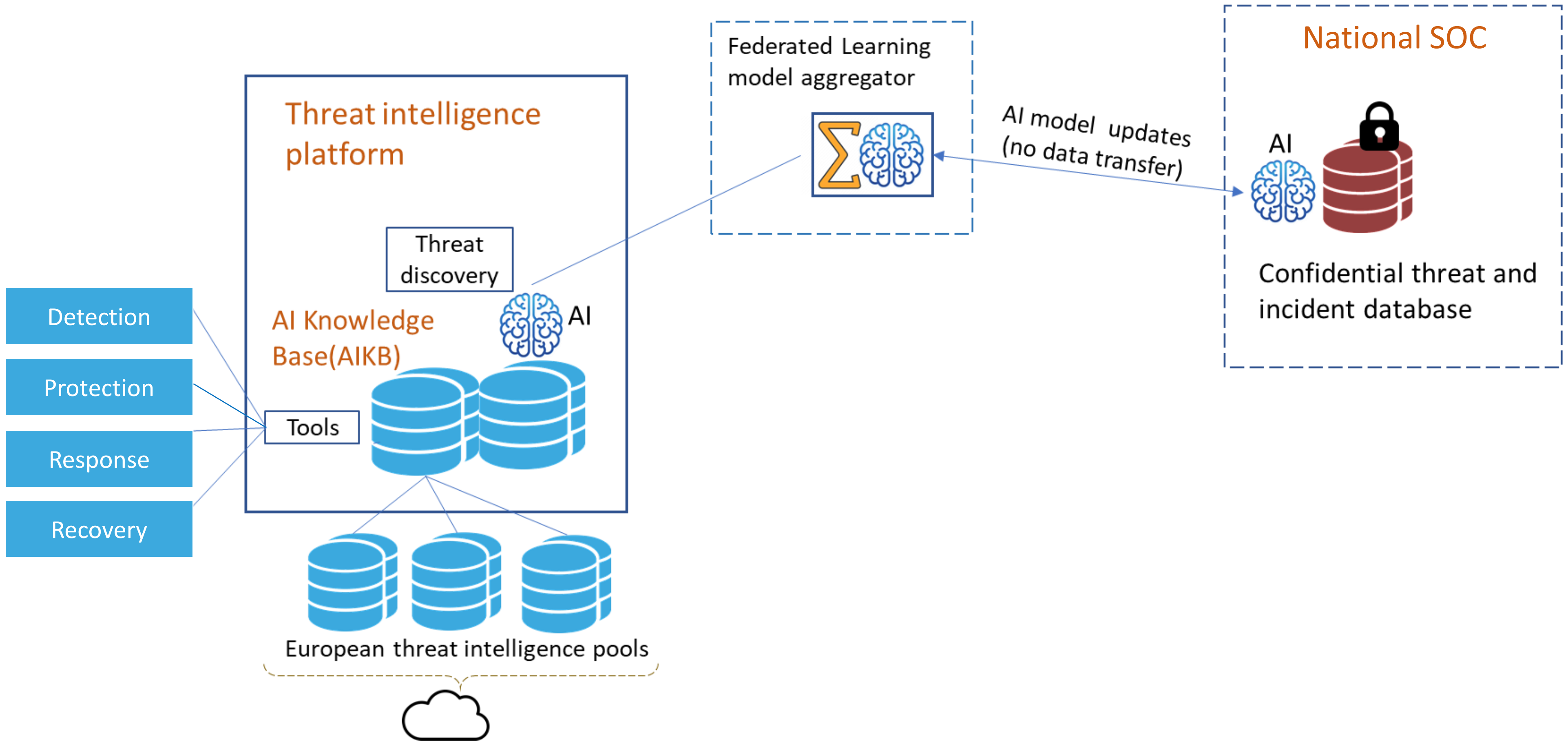
#	ORGANISATION	PRESENTER
1	Gradiant	Lilian Adkinson Orellana
2	Binalyze	Klaus-Peter Finke-Härkönen
3	XaaS Enterprise GmbH	Juergen Kreuz
4	SAMA PARTNERS	Mael Pegny
5	TUV Austria	Grigore Stamatescu
6	Sourceline	Teodor Pricop

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH
Novel applications of AI and Other Enabling Technologies for Security Operation Centres

Lilian Adkinson Orellana (ladkinson@gradiant.org)
Head of security and privacy analytics

Gradiant (RTO, Spain)
WP leader, R&D tasks

DIANA - enhanceD cyber threat Intelligence on a privAcy preserviNg and federAted Computation



Threat intelligence platform
Threat discovery
AI Knowledge Base(AIKB)
AI
Tools
Detection
Protection
Response
Recovery
European threat intelligence pools
Federated Learning model aggregator
AI model updates (no data transfer)
National SOC
AI
Confidential threat and incident database

DIANA - enhanceD cyber threat Intelligence on a privAcy preserviNg and federAted Computation

- Development of a FL based platform for the distributed training of AI models among National SOCs in a private preserving manner, and generation of CTI.
- The platform will include also a cybersecurity toolset, composed by:
  - **Tools for threat detection and anomaly identification**, enabling real time monitoring as well as early incident warning: anomaly detection tool, UEBA (User and Entity Behaviour Analytics), process mining tool, digital image forensics, biometrics.
  - **Tools for the sharing of CTI and other sensitive data:** data anonymization tool, as well as other cryptographic and non cryptographic PETs (Privacy Enhancing Techniques).
  - **Tools for vulnerability management**, including their identification, automatic scanning solutions and penetration testing.
  - **Tools for the mitigation of threats**, and the enabling of a rapid response and recovery, including malware.

Project participants

Partners:

- Gradiant (Spain –WP/task leader, R&D):
  - Anomaly detection
  - UEBA (User and Entity Behaviour Analytics)
  - Process mining
  - Anonymization
  - Other PETs (Privacy Enhancing Technologies)
  - Digital image forensics
  - Biometric recognition

Looking for partners with the following expertise:

- Vulnerability management
- Vulnerability scanning
- Response and recovery
- National SOCs

b!nalyze

A Novel Cyber Incident Response Investigation Platform Automating Forensics in Enterprise Security Operation Centres (SOC)

NIS2 COMPLIANCE AUTOMATION:

Cyber Hygiene
Cyber Incident Handling
Cyber Incident Reporting

Binalyze OÜ
14434021
Tallinn, Estonia

Molten

cisco investments

citi VENTURES

Deutsche Bank

DIGITAL EAST FUND

OpenOcean

Forensically Sound Cyber Incident Handling & Reporting

b!nalyze

2024 ECSO CISO Choice Award Finalist

b!nalyze

Automating Forensics in Security Operation Centres

ECHO Project

Grant agreement ID: 830943

Binalyze was a participant, which informed development of our fit-for-purpose solution enabling enterprises to meet NIS2 cyber incident reporting requirements

LOCARD Project

EC Grant agreement ID: 832735

Binalyze validated for Cross Border Chain of Custody in today's Global Cyber Law Enforcement Operations

BlockChain + Binalyze AIR

European & Certified

Established 2018 in **Estonia**

ISO/IEC 27001
ISO/IEC 27701
ISO/IEC 27017
ISO/IEC 27018

b!nalyze

We are seeking to partner with National Coordination Centres (NCCs), Academic Instituitions and Managed Security Service Providers (MSSPs) to integrate our Binalyze AIR Platform into:

- Open Standards based Cyber Threat Intelligence (CTI) sharing frameworks (MISP, STIX)
- Automated Incident Recovery (Self Healing) proposed frameworks (OASIS OPEN CACAO)

Contact: klaus@binalyze.com

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

SECaaS.IT
Security as a Service

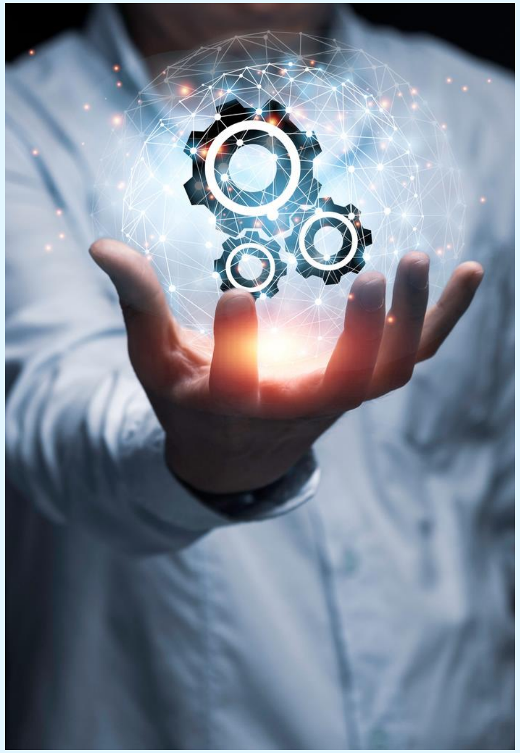
SECaaS PRISM Tool

Funding Call

DIGITAL-ECCC-2024-DEPLOY-CYBER

06-ENABLINGTECH

Jürgen Kreuz - CEO XaaS Enterprise GmbH - SECaaS.IT
Bucharest - 22.02.2024



SECaaS – Security as a Service
+49-69-5060-7820

JK@SECaaS.IT

Jürgen Kreuz

Over 100 completed ISO, NIS 2, DORA, CRA and IT-Compliance assignments for medium and large businesses in the critical infrastructure sector, particularly healthcare.

Organisation

IT SECURITY

Technology

People

"The best possible security for our customers"

Unified Goal

Commitment

Expertise

Reliability

Partnership

SECaaS.IT
Security as a Service

DIGITAL-ECCC-2024-DEPLOY-CYBER 06-ENABLINGTECH

SECAAS PRISM

Critical infrastructure sectors lack a unified solution that simplifies and enhances compliance, cyber-security monitoring, and management.

This makes it challenging to effectively address security threats and regulatory demands simultaneously.

A Comprehensive IT Security Journey from ISO27001 Implementation to an AI-Powered SOC for Advanced Threat Defense

PRISM 4 ISO

Foundation for an ISMS compliant with ISO 27001, laying the groundwork for cyber-security standards and regulatory compliance. Expands to include ISO 9001, GDPR, DORA, and CRA, with local enhancements like C5 in Germany.

PRISM MODULES

Expansion modules enhancing the core ISMS framework. Includes extensions to various ISO standards and regulatory requirements, enabling a customizable approach to compliance and security management.

PRISM+

Introduces AI-driven processes for documenting and enhancing IT security workflows. Integrates monitoring data from tools like XDR and regressive pentesting tools, alongside other cyber-security software

AI

PRISM PREMIUM

Evolves into an automated, AI-powered SIEM, providing advanced monitoring, threat detection, and incident response. Streamlines security operations for efficiency and enhanced threat defense.

AI

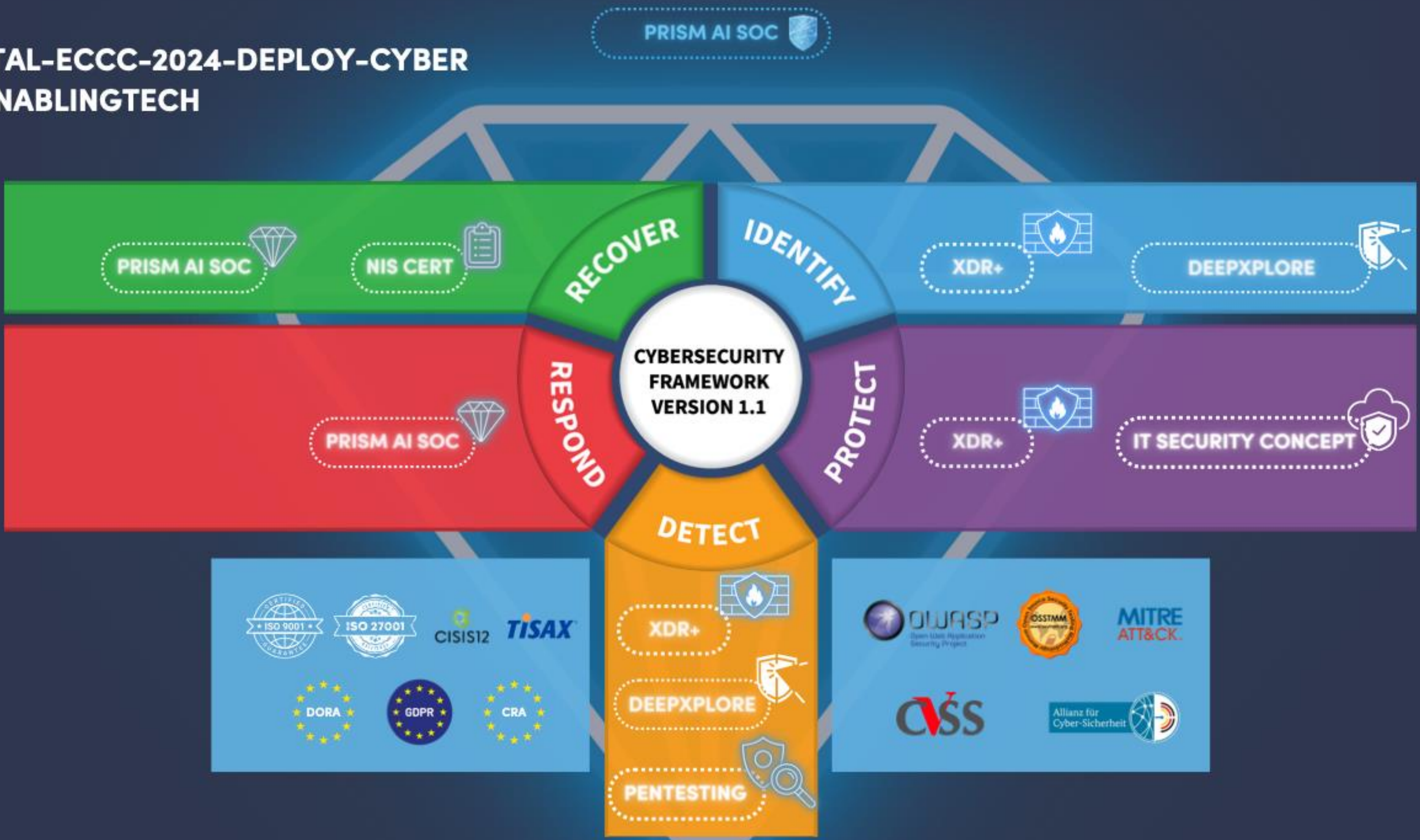
PRISM AI SOC

The pinnacle of IT security solutions, establishing an AI-powered Security Operations Center (SOC) for the highest security demands. Offers proactive threat hunting and advanced defense capabilities.

AI

SEC✓aaS.IT
Security as a Service

DIGITAL-ECCC-2024-DEPLOY-CYBER 06-ENABLINGTECH



SECaaS.IT Security as a Service

WOLFPACK

COLLEGIUM AUDITORES MALTA Limited

ATTHENE GPT

U-Know

Adornis

CYTRES

SECAAS PRISM

Roadmap

Critical Infrastructure Pilot running with:

St.-Johannes-Hospital
Schwerpunktkrankenhaus
Kath. St.-Johannes-Gesellschaft Dortmund gGmbH

PRISM 4 ISO

March 2024

PRISM 4 ISO

Within the first Quarter of 2024 we are establishing the PRISM 4 ISO Solution in the market and will use the basis for our clients

April 2024

PRISM Modules

First Standards, such like C5 of BSI, DORA and ISO 9001 will be added to the PRISM basis

PRISM MODULES

PRISM MODULES

June 2024

PRISM Pilot

Establishment of certain components of PRISM AI SOC at our Pilot customer: a hospital in Dortmund

June 2024

PRISM+ Beta

The process component will be established in the Pilot project and will be qualified for commercial use.

PRISM+

PRISM+

August 2024

PRISM+ Impl.

First commercial implementation of the PRISM+ version.

PRISM PREMIUM

September 2024

PRISM Premium

First implementation of PRISM Premium during the Pilot installation at our Pilot hospital and qualification for commercial use.

PRISM AI SOC

December 2024

AI SOC Beta

Implementation of a Beta AI Soc at our Pilot customer and qualification for further development and additional POCs

PRISM AI SOC

March 2025

PRISM AI SOC

Commercial Go to Market for PRISM AI SOC for target markets.

Jürgen Kreuz
+49 171 4784266
JK@SECaaS.IT

SECaaS.IT
Security as a Service

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

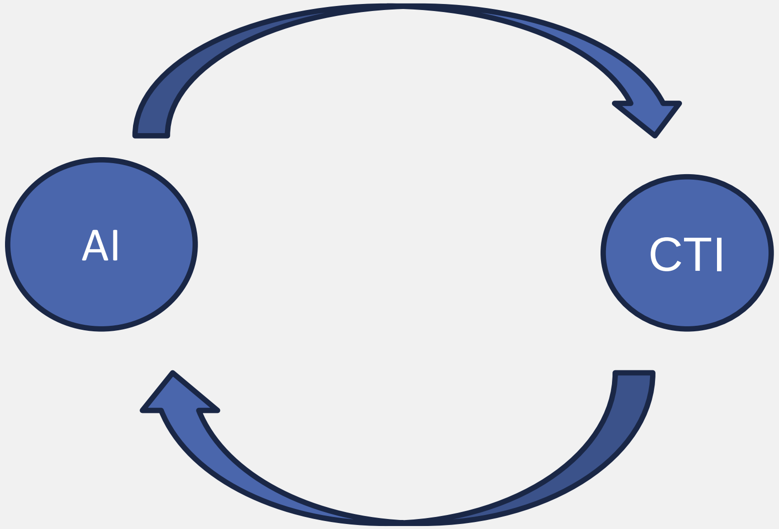
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

AI-Enhanced Deception for CTI

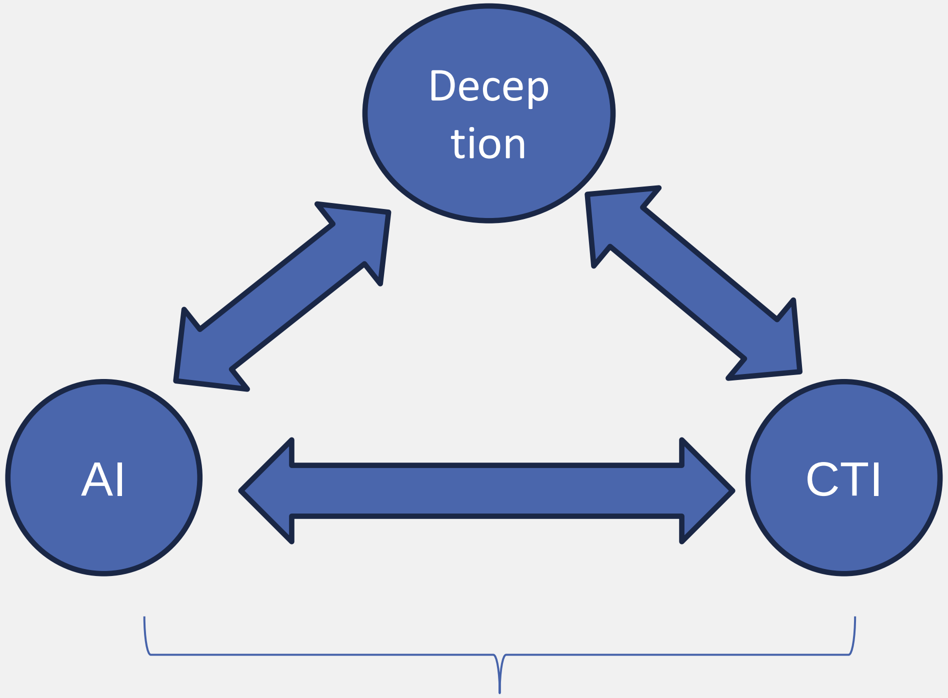
Maël Pégny ECCC Info-Day, Feb.22, 2024. Bucharest

Strengthening AI & CTI with a Third Player: Deception

Our common starting point



SAMA PARTNERS PROJECT



Deceptionrange

Cyberdeception as Enhancement for AI & CTI

Cyberdeception & AI

AI intervenes throughout the deception chain:

- **1: Fake data generation**
- **2: Optimal dynamic environment tailored to adversary's characteristics & reactions**
- **3. Automated Analysis for real-time reactivity**
- **4. Big Data Analysis feeding back into 1&2, classical CTI functions and AI models for cybersecurity**

Cyberdeception for CTI Collection & Analysis

Cyberdeception as unique environment for CTI collection:

- **Live action monitoring vs forensics-based CTI**
- **Timely & relevant intel by construction**
- **Safe environment tailored for data collection**
- **Prevention of evidence erasure**
- **Prompting adversary with tailored environment to elicit behavior revealing evidence high on the PoP: from CTI collection to CTI elicitation**

Turning the trap into a DeceptionRange!

Our Input: Dynamic Deception for CTI in Europe

Top cyberdeception companies: dominated by USA and Israel

- **Only two European exceptions:**
  - **Cybertrap (Austria) → Great monitoring abilities, but no dynamic deception (GigaOM'23 report)**
  - **Lupovis (UK) → ML-driven, pre-and-post breach gamified deception for CTI elicitation**

- **Our offer: combining dynamic deception and advanced CTI collection environment leveraging our company strengths:**
  - **Experience as SOC provider**
  - **Multi-branch experience**
  - **In-house cyberrange**
  - **Integration of recent research on cognitive bias (cybermanoeuvers, J. MacKneely)**
  - **CTI useful for law enforcement & intelligence services to neutralize hackers, strengthening the whole EU ecosystem.**

Wealth of data

OPEN TO COLLABORATION WITH ACADEMIA & PUBLIC SECTOR!
mael.pegny@samapartners.com

TÜV AUSTRIA

Cross-border Energy SOC with AI-enhanced Cognitive and Real-Time Capabilities

Dr.-Ing. Grigore Stamatescu | ECCC Info Day, 22 February 2024, Bucharest

CONTEXT

- ✓ Active since 2007, 160+ employees, 20Mio+ EUR turnover, part of TUV Austria Group
  - Cybersecurity portfolio: cybersecurity audits, ISO27001 certification and training
- ✓ Partner in two Horizon 2020 R&D projects:
  - The Food Safety Market: an SME-powered industrial data platform to boost the competitiveness of European food certification (TheFSM), 2020 – 2023
  - rEsilient and seLf-healed EleCTRical pOwer Nanogrid (ELECTRON), 2021 – 2024 https://electron-project.eu/
- ✓ Focus on ELECTRON
  - Key Technologies: Intrusion detection (SIEM), Anomaly detection using Federated Learning (FL-IDPS), Cyberthreat Intelligence (Threat Explorer), MISP-based repository (SharePoint), PQC
  - WP leader for regulation and policy making (CSA, NIS2, CER, NCCS, CRA), EU information exchange and standardisation

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

- ✓ Novel applications of AI and Other Enabling Technologies for Security Operation Centres
- ✓ Relevant aspects
  - Continuous detection of patterns and identification of anomalies that indicate potential threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape
  - Enhancing speed of incident response through real-time monitoring of networks to identify security incidents and generating alerts or triggering automated responses.
  - Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymisation and de-identification

- ✓ Reference to ENISA Artificial Intelligence and Cybersecurity Research Report – June 2023

IDEAS / PROPOSAL

- ✓ **Deployment of a cross-border SOC using state-of-the-art developments in AI for the energy sector**
- ✓ Design, implementation and operationalization of the cross-border energy SOC
- ✓ Integration and development of both open-source (e.g. from cybersecurity clusters) and proprietary AI technologies
- ✓ Domain-specific knowledge from IACS and Energy sectors to enhance AI models, systems and tools
- ✓ Standards-based approach e.g. ISO 27019, IEC 62443
- ✓ Support for compliance with NIS2 and NCCS
- ✓ SOC federations for trustworthy anonymized CTI sharing and support of National SOC objectives
- ✓ Tentative consortium: MSSPs, tools and service providers (SME/Start-Up – France, Large Company - Spain), academia (Romania, Greece, Spain – including HPC), EU-wide organisations (EE-ISAC), representative end-users from the energy sector (Producers, TSOs, DSOs)

Data Access Protection

Protecting sensitive data through the analysis of access patterns and detection of abnormal behaviour.

Novel applications of AI and other enabling technologies for security operation centres

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

Teodor Pricop
office@sourceline.ro

sourceline

What is sensitive data?

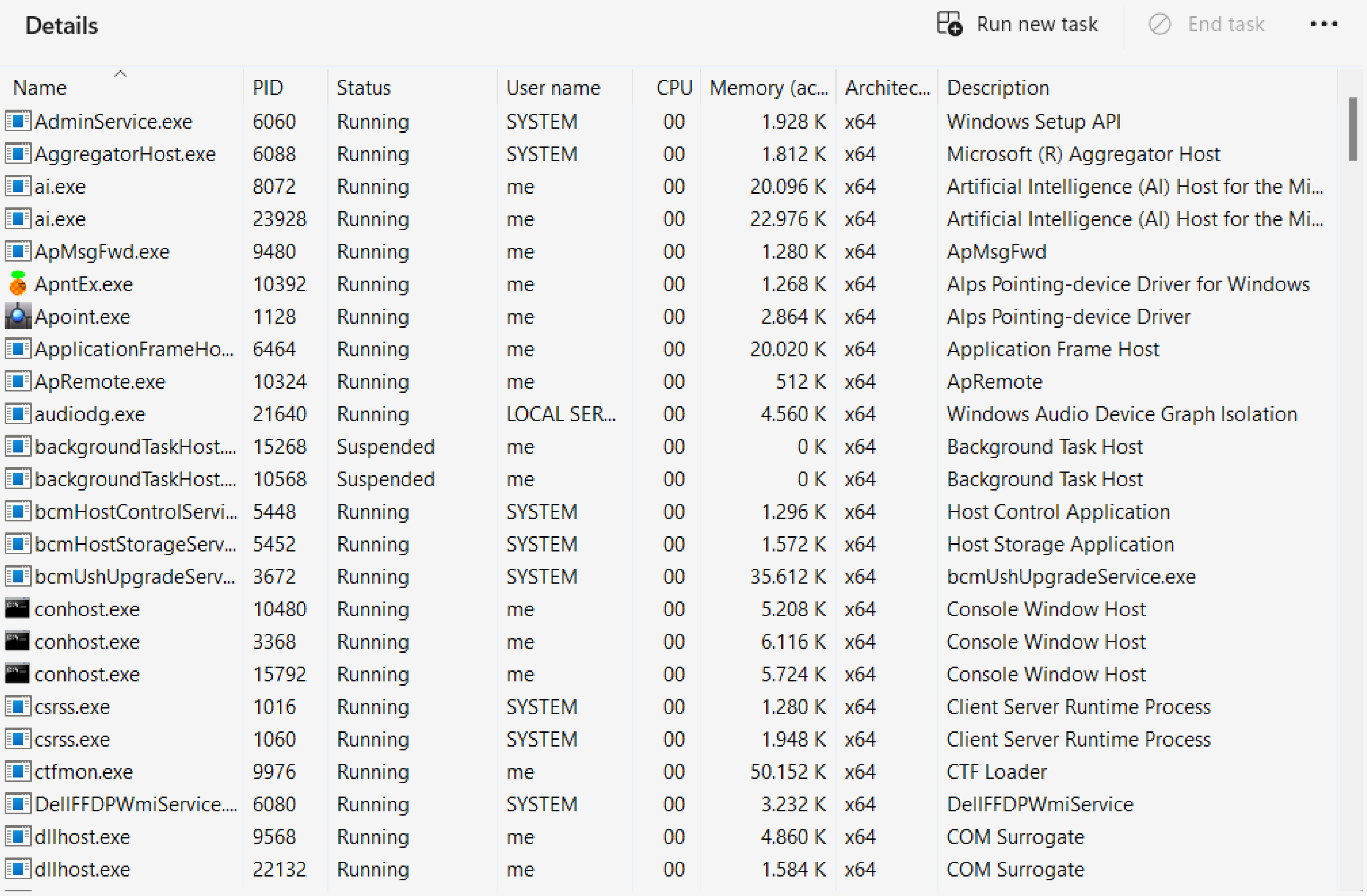
Supplier List.xlsx

Financial operations.docx

Client Information.xlsx

Q3 Results.pptx

Who can access my data?



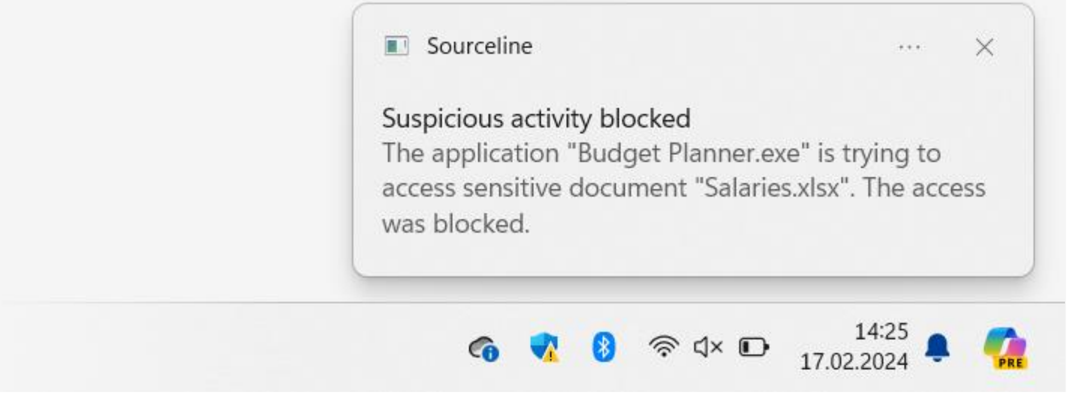
Name	PID	Status	User name	CPU	Memory (ac...	Architec...	Description
AdminService.exe	6060	Running	SYSTEM	00	1.928 K	x64	Windows Setup API
AggregatorHost.exe	6088	Running	SYSTEM	00	1.812 K	x64	Microsoft (R) Aggregator Host
ai.exe	8072	Running	me	00	20.096 K	x64	Artificial Intelligence (AI) Host for the Mi...
ai.exe	23928	Running	me	00	22.976 K	x64	Artificial Intelligence (AI) Host for the Mi...
ApMsgFwd.exe	9480	Running	me	00	1.280 K	x64	ApMsgFwd
ApntEx.exe	10392	Running	me	00	1.268 K	x64	Alps Pointing-device Driver for Windows
Apoint.exe	1128	Running	me	00	2.864 K	x64	Alps Pointing-device Driver
ApplicationFrameHo...	6464	Running	me	00	20.020 K	x64	Application Frame Host
ApRemote.exe	10324	Running	me	00	512 K	x64	ApRemote
audiodg.exe	21640	Running	LOCAL SER...	00	4.560 K	x64	Windows Audio Device Graph Isolation
backgroundTaskHost....	15268	Suspended	me	00	0 K	x64	Background Task Host
backgroundTaskHost....	10568	Suspended	me	00	0 K	x64	Background Task Host
bcmHostControlServi...	5448	Running	SYSTEM	00	1.296 K	x64	Host Control Application
bcmHostStorageServ...	5452	Running	SYSTEM	00	1.572 K	x64	Host Storage Application
bcmUshUpgradeServ...	3672	Running	SYSTEM	00	35.612 K	x64	bcmUshUpgradeService.exe
conhost.exe	10480	Running	me	00	5.208 K	x64	Console Window Host
conhost.exe	3368	Running	me	00	6.116 K	x64	Console Window Host
conhost.exe	15792	Running	me	00	5.724 K	x64	Console Window Host
csrss.exe	1016	Running	SYSTEM	00	1.280 K	x64	Client Server Runtime Process
csrss.exe	1060	Running	SYSTEM	00	1.948 K	x64	Client Server Runtime Process
ctfmon.exe	9976	Running	me	00	50.152 K	x64	CTF Loader
DellFFDPWmiService....	6080	Running	SYSTEM	00	3.232 K	x64	DellFFDPWmiService
dllhost.exe	9568	Running	me	00	4.860 K	x64	COM Surrogate
dllhost.exe	22132	Running	me	00	1.584 K	x64	COM Surrogate

Our solution

1. Identify access requests to **sensitive data**

2. Separate **user actions** from background tasks using AI

3. Allow only **legitimate access requests** initiated by the user



Sourceline

Suspicious activity blocked
The application "Budget Planner.exe" is trying to access sensitive document "Salaries.xlsx". The access was blocked.

14:25
17.02.2024

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA
Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations

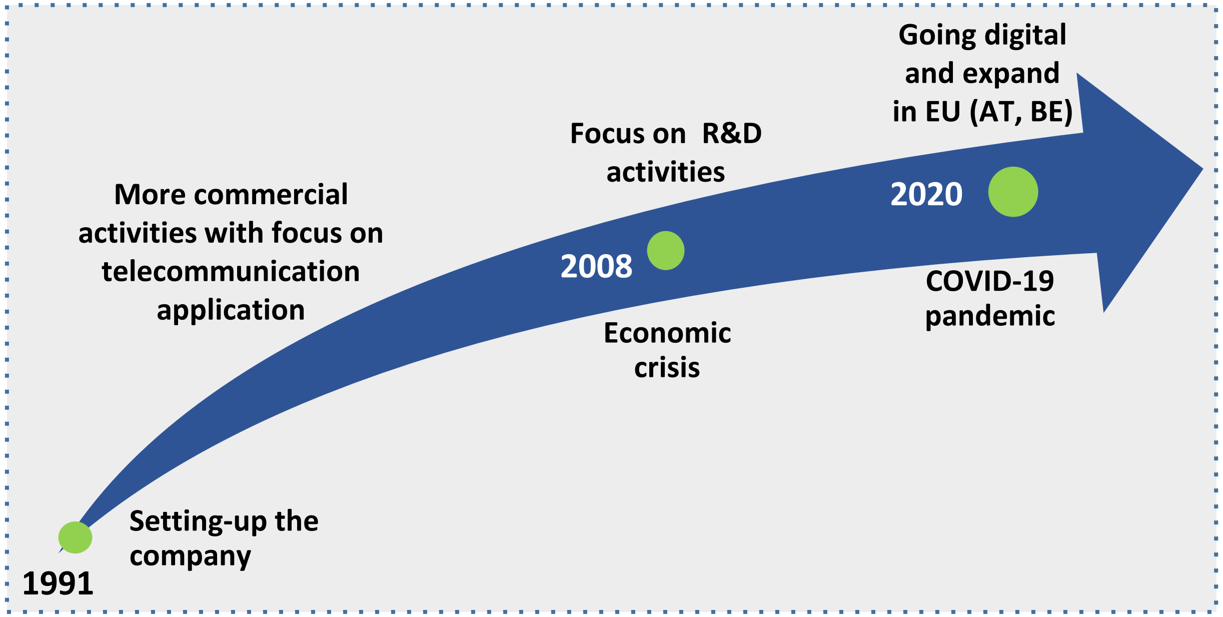
#	ORGANISATION	PRESENTER
1	Beia	George Suciu

DIGITAL ECCC Info Day
22 February 2024

Experience in Cyber-Physical Security Projects

George Suciu
BEIA CONSULT INTERNATIONAL SRL
george@beia.eu
Twitter: @GeorgeSuciuG

General Business Description



1991

Setting-up the company

More commercial activities with focus on telecommunication application

2008

Focus on R&D activities

Economic crisis

2020

Going digital and expand in EU (AT, BE)

COVID-19 pandemic

BEIA team

89 persons
- 30 engineers, 10 technicians
- 20 R&D employees (5 Prof, 5 PhD, 4 medical doctors)
- 12 in sales and marketing
- 5 in economic, HR& management

R&D Innovation projects (over 60)

EU - Horizon, Eureka Clusters, ERA-NET, Eureka network, Eurostars, etc.

National – National Research Programs, Operational programs, etc.

Expertise of the R&D Department: BEIA is a R&D performing SME with focus on time critical Artificial Internet of Things (AIoT) and a team with experience in R&D **service innovation** (AI, blockchain, cloud, big data, cyber-physical & quantum security), **hardware integration** (sensors, actuators, IoT), information technologies (data analytics, back end, interfaces, front end), integration (software/hardware), communication technologies (speech processing, sentiment analysis, emotional computing), communication/ dissemination/marketing, project management.

Experience related to the call:

- Awareness raising, disseminaton and managing open call as EDIH from previous projects such as ADMA, WeH, DOME, HUBCAP, SHIFT-HUB, ECYBRIDGE
- Contacts with manufacturers of products with digital components, providers of CRA stakeholders, FOSS

Partnerships

- Partners in Romanian R&D:
  - Research and Academia
    - University “POLITEHNICA” of Bucharest (www.upb.ro)
    - Constanta Maritime University (www.cmu-edu.eu)
    - Ovidius University of Constanta (www.univ-ovidius.ro)
    - Research Institute for Artificial Intelligence at the Romanian Academy (www.racai.ro)
    - Romanian Space Agency (www.rosa.ro)
    - National Institute for Research and Development in Electrical Engineering (www.icpe-ca.ro)
    - National Institute of Aerospace Research “ELIE CARAFOLI” (www.incas.ro)
    - National Institute for Research and Development in Informatics (www.ici.ro)
    - Institute for Research and Development in Automation (www.ipa.ro)
    - The Romanian Academy –”Stefan S. Nicolau” Institute of Virology (www.virology.ro)
    - University of Medicine and Pharmacy “Carol Davila” Bucharest (www.umfcd.ro)
    - University of Agronomic Sciences and Veterinary Medicine of Bucharest (www.usamv.ro)
    - Research and Development Institute for Industrializing and Marketing Horticulture Products “HORTING” (www.horting.ro)
    - National Institute for Research and Development in Microbiology and Immunology for the Military (www.cantacuzino.ro)
  - critical infrastructure operators "**CI**"
    - telecom, finance, food, energy (DSO, SG/RES/ESS, EV/PV, nuclear), water (ports, shipping), transport (metro/railway), chemical industry, RI, etc.
  - first responder organizations "**FRO**"
    - firefighters, ambulance, red cross, volunteer organizations, SMURD, forensic investigators, crime scene investigators, CERT/CSIRT, etc.
  - law enforcement agencies "**LEA**"
    - police, border guard, customs, environmental guard, coast guard, ports administration, STS, SPP, SRI, other authorities from the Ministry of Interior, Ministry of Defense, etc.
- Founding Member in the Directory Council of the German-Romanian Chamber of Industry and Commerce (AHK-Deutsch-Rumaenische Industrie- und Handelskammer) and member of other Chambers of Commerce
- Leader of NEM Romanian Mirror Group (www.nem-pt.ro) and ARTEMIS
- Member of Romanian Association for Electronic and Software Industry (ARIES), Electronic Innovation Cluster (ELINCLUS), MHTC, DRIFMAT, ICONIC, IND-AGRO-POL, ROHEALTH, H2ROMANIA, PROECO – CBRNE, EARSC, ITEA, Celtic, 5G-PPP, PATROMIL, PRO-NZEB, AIOTI, BDVA, 6G-IA, etc.

Security Related R&D PROJECTS

- **Energy**
  - **SealedGRID**: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID
  - **BENTRADE**: Blockchain Based Energy Distribution & Trade Platform
  - **I-DELTA**: Interoperable Distributed Ledger Technology
  - **MULTISCALE**: Research on the development of advanced materials and multiscale optimization by integrating nano-structured materials into advanced energy systems
- **Smart Cities**
  - **CHRISS**: Critical infrastructure High accuracy and Robustness increase Integrated Synchronization Solutions (HORIZON CL4 EUSPA-2021-SPACE-02-52)
  - **MOBILISE**: A novel and green mobile One Health laboratory for (re-) emerging infectious disease outbreaks (HORIZON EUROPE CL3)
  - **FLEXI-CROSS**: Flexible and Improved Border-Crossing Experience for Passengers and Authorities (HORIZON EUROPE CL3)
  - **RITHMS**: Research, Intelligence and Technology for Heritage and Market Security (HORIZON EUROPE CL3)
  - **CyberSec2SME/SecureIT** - CONTINUOUS CYBER SECURITY AUDIT (H2020 open call)
  - **SAFECARE**: SAFEguard of Critical heAlth infrastructure
  - **S4AllCities:** Smart Spaces Safety and Security for All Cities
  - **STAMINA:** Demonstration of intelligent decision support for pandemic crisis prediction and management within and across European borders
  - **DEFRAUDify**: Detect Fraudulent Activities in dark web and clear web to protect your business
  - **SCRATCh:** SeCuRe and Agile Connected Things
  - **ENTA:** Encrypted Network Traffic Analysis for Cyber Security
  - **PARFAIT:** Personal dAta pRotection FrAmework for IoT
  - **AICom4Health**: AI-Powered Communication for Health Crisis Management (Celtic)
- **Industry**
  - **ECYBRIDGE**: Strengthening Synergies in Defence and Civilian Cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE)
  - **PASITHEA:** A Hybrid Autonomous Unmanned Vehicle system opening new horizons in conducting military operations in the marine environment (EDF)
  - **AIAS:** AI-ASsisted cybersecurity platform empowering SMEs to defend against adversarial AI attacks (HORIZON MSCA)
  - **VITAL-5G**: Vertical Innovations in Transport And Logistics over 5G experimentation facilities (H2020 ICT-41)
  - **FOR-FREIGHT**: Flexible, multi-mOdal and Robust FREIGHt Transport (HORIZON EUROPE CL5)
  - **ADMA TranS4MErs**: Advanced Manufacturing assistance and training for SME Transformation (H2020 INNOSUP CSA)
  - **Arrowhead Tools**: Arrowhead Tools for Engineering of Digitalisation Solutions
  - **EREMI**: Education for Resource Efficency in Manufacturing Industries
  - **UPSIM**: Unleash Potentials in Simulation
  - **SWAM**: Smart WAter Management system for better environmental sustainability
  - **PIMEO AI**: Pollution Identification, Mapping, and Ecosystem Observation with AI-powered water quality USV
  - **MIHA:** An Affordable Humanoid Platform for Research and Development (EIT Digital InnovationFactory)
  - **DISTINGO**: RECONFIGURABLE SMART LOCKERS - DISTributeurs INtelliGents recOnfigurables (Celtic)
- **AGRI-FOOD**
  - **FarmSustainaBl:** Enabling Smart Livestock Farming Technologies for Environmental Sustainability using Blockchain
  - **ADCATER / Food-Friend**: Advanced Digital Solutions for Professional Food and Nutrition Catering Service
  - **SMARTCHAIN**: Smart solutions for advancing supply systems in blue bioeconomy value chains (ERA-Net BlueBio)
  - **SmartVIT/IoT-NGIN:** Smart Viticulture Management system for better environmental sustainability project (H2020 open call)
  - **NGI-UAV-AGRO:** Next Generation Internet based on 5G and UAV for precision agriculture (PED), 2020-2022;

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA
Tools for compliance with CRA requirements and obligations

#	ORGANISATION	PRESENTER
1	Eclipse Foundation	Mikael Barbero & Enzo Ribagnac
2	CybrOps	Adrian Ifrim
3	Zepo	Antonio Munoz
4	Cyber Cert Labs	Patricia Shields

Enzo Ribagnac <enzo.ribagnac@eclipse-foundation.org>
Associate Director, European Public Policy
Mikael Barbero <mikael.barbero@eclipse-foundation.org>
Head of Security

SME Open Source Compliance Toolkit

DIGITAL-ECCC-2024-DEPLOY-CYBER-06 -COMPLIANCE CRA

€8,17 trillion

Open Source value, if companies were to pay for it

Source:
Harvard Business School

80% to 90%

of digital products are made of Open Source Software

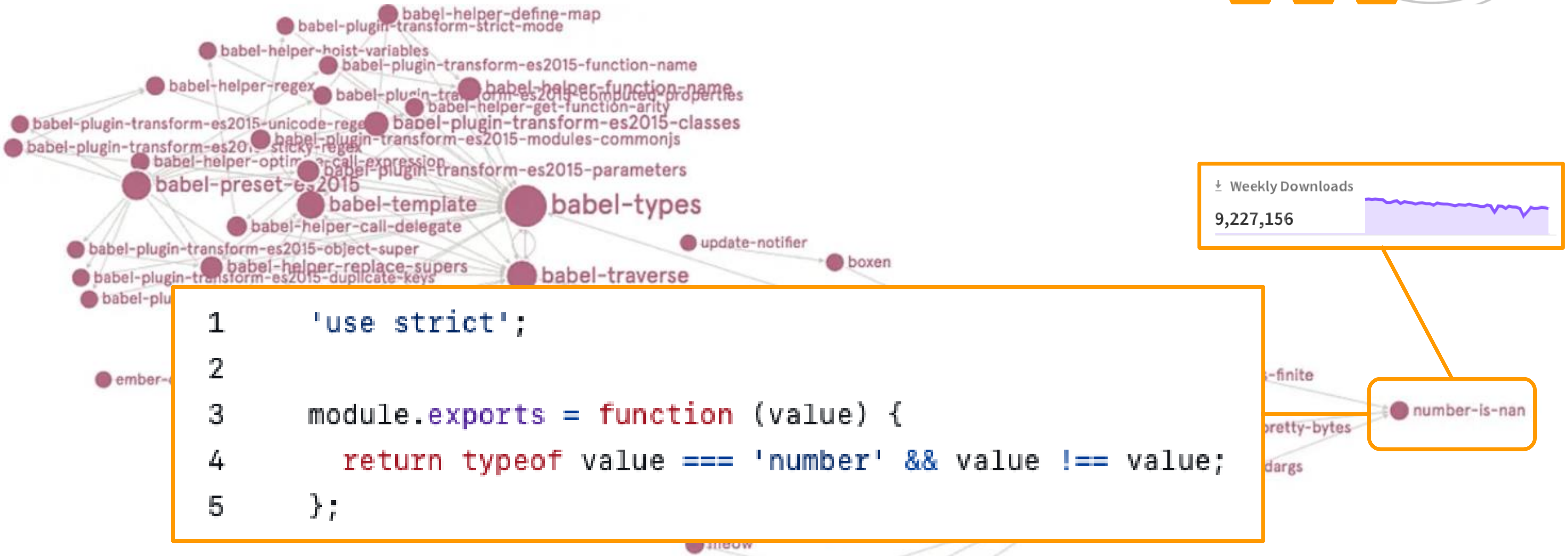
Source:
Forrester

Open source appears in **96%** of codebases & up to **99.9%** of components of commercial software

Source:
Musseau et al., & Synopsys

ECLIPSE® FOUNDATION

An SME struggle: document and assess OSS


babel-helper-define-map
babel-plugin-transform-strict-mode
babel-helper-hoist-variables
babel-plugin-transform-es2015-function-name
babel-helper-regex
babel-plugin-transform-es2015-computed-properties
babel-helper-function-name
babel-helper-get-function-arity
babel-plugin-transform-es2015-unicode-regex
babel-plugin-transform-es2015-classes
babel-plugin-transform-es2015-sticky-regex
babel-plugin-transform-es2015-modules-commonjs
babel-helper-optimise-call-expression
babel-plugin-transform-es2015-parameters
babel-preset-es2015
babel-template
babel-types
babel-helper-call-delegate
update-notifier
babel-plugin-transform-es2015-object-super
boxen
babel-helper-replace-supers
babel-plugin-transform-es2015-duplicate-keys
babel-traverse
babel-plu
ember-
-finite
number-is-nan
pretty-bytes
dargs
meow

Weekly Downloads

9,227,156

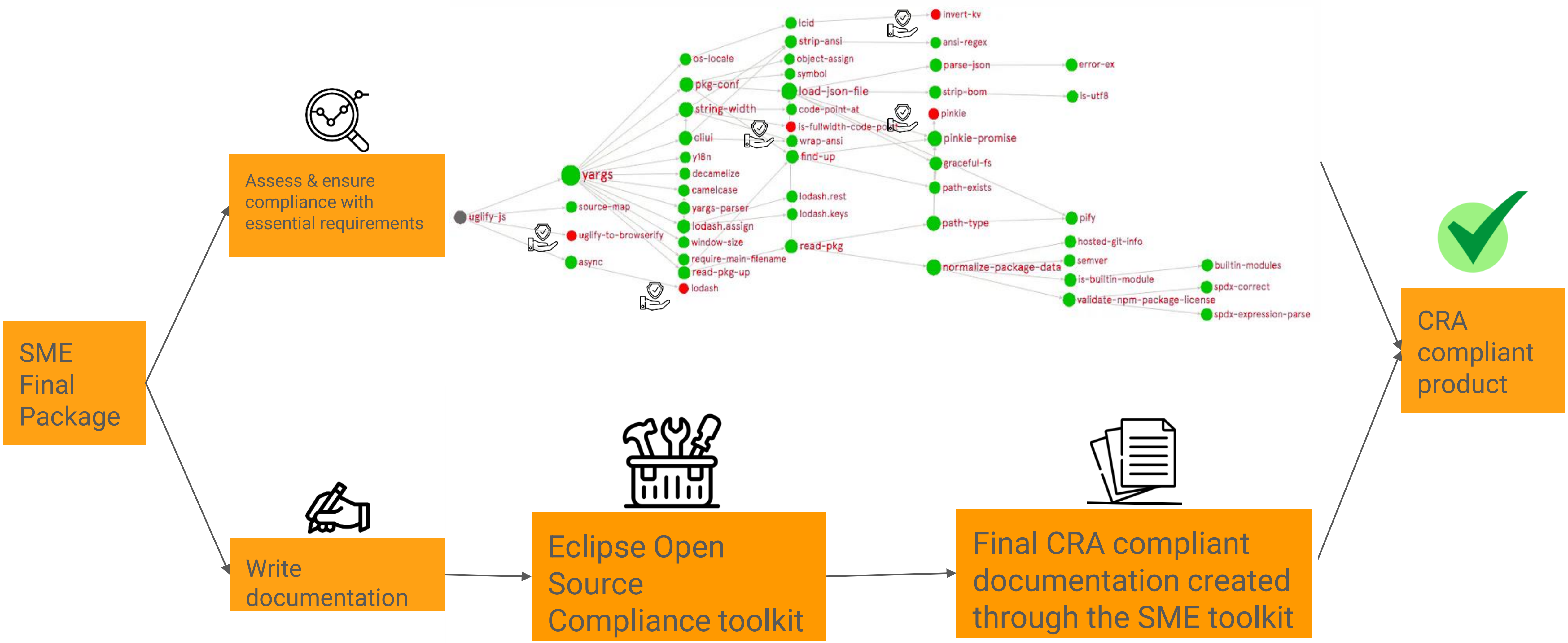
```
'use strict';

module.exports = function (value) {
  return typeof value === 'number' && value !== value;
};
```

No SME can comply with the CRA on documentation and essential requirements, without assessing open source components during design, development and production of products with digital elements

Article 10(1), 10(4), 23(1), Annex 1, Annex 5 of the CRA

SME Compliance toolkit



SME Final Package

Assess & ensure compliance with essential requirements

Write documentation

Eclipse Open Source Compliance toolkit

Final CRA compliant documentation created through the SME toolkit

CRA compliant product

Robust Consortium Powered by SMEs

- Hundreds of SMEs from Europe are currently members of Eclipse Foundation.
- Work will be split with half a dozen of SMEs, to develop tools in domain they have expertise.
- A dozen will provide use cases, and demonstrate benefits from the implemented tools and processes.
- Collaboration with other high profile Open Source Foundations
- Collaboration with SME associations for the creation of a series of events and communication to disseminate the knowledge of the toolkit.
- Collaboration with several NCCs across Europe to ensure alignment of the toolkit with CRA enforcement as well as communication and dissemination.

Cyber Security Redesigned

Shifting the focus from effort to performance

We are on a mission to transform the way organizations reach and maintain digital operational resilience

Current state

- Ineffective cyber defense strategies
- No holistic approach that offers a bird eye overview
- Lack of critical up-to-date data for decision makers
- Insufficient capabilities for compliance with internal and external regulations

CybrOps

CybrOps proposal

- A shift in focus from effort to **performance** and capabilities to measure success
- Real-time integration of efforts and **collaboration** in a distributed environment
- Data based decisions for digital operational **resilience**

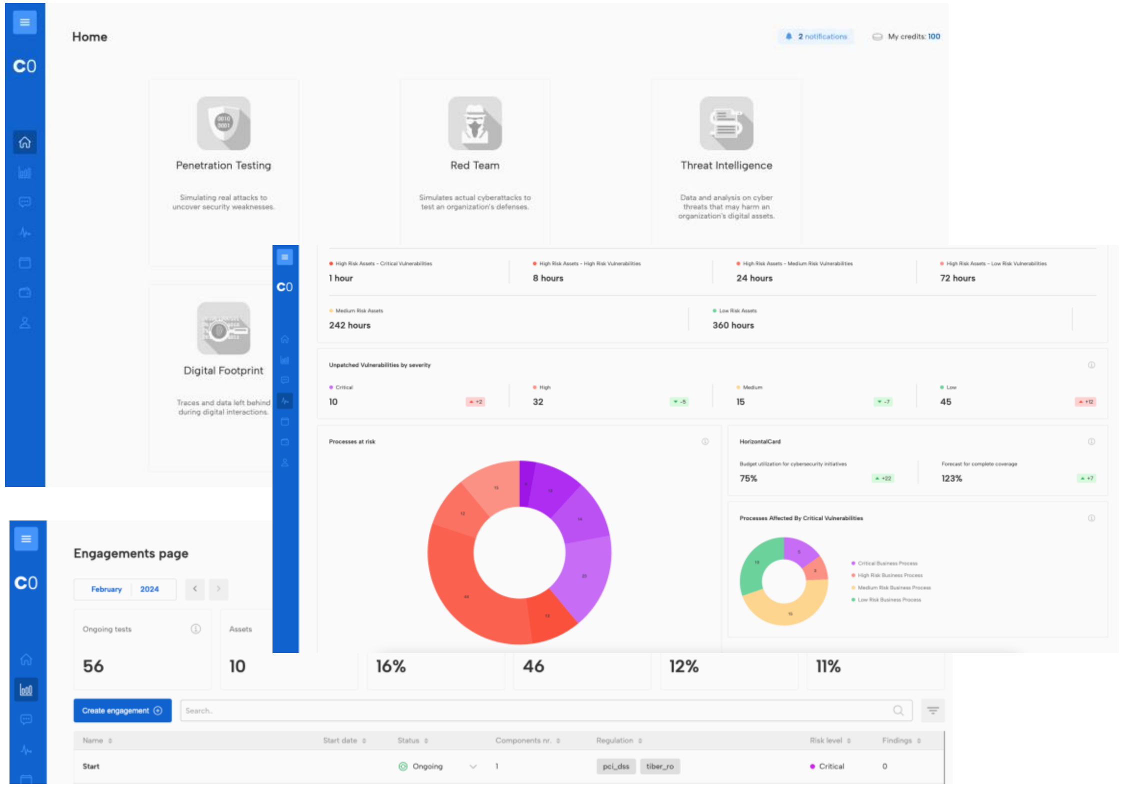
CybrOps

CybrOps platform

e. adrian.ifrim@cybrops.io
t. +40 734 701 487
w. cybrops.io

e. cristian.mocanu@cybrops.io
t. +40 722 626 877
w. cybrops.io

- Battlefield tested
  - faster delivery time
  - projects real-time status
- Factfulness
  - data-driven decision making
  - relevant KPI
- Compliance
  - external regulations
  - internal requirements
- Gamification
  - rewarding talent
  - improving engagement


CO
Home
2 notifications
My credits: 100
Penetration Testing
Simulating real attacks to uncover security weaknesses.
Red Team
Simulates actual cyberattacks to test an organization's defenses.
Threat Intelligence
Data and analysis on cyber threats that may harm an organization's digital assets.
Digital Footprint
Traces and data left behind during digital interactions.
Processes at risk
HorizontalCard
Processes Affected By Critical Vulnerabilities
Critical Business Process
High Risk Business Process
Medium Risk Business Process
Low Risk Business Process
Engagements page
Create engagement
Search..

High Risk Assets - Critical Vulnerabilities: 1 hour
High Risk Assets - High Risk Vulnerabilities: 8 hours
High Risk Assets - Medium Risk Vulnerabilities: 24 hours
High Risk Assets - Low Risk Vulnerabilities: 72 hours
Medium Risk Assets: 242 hours
Low Risk Assets: 360 hours

Unpatched Vulnerabilities by severity
Critical 10 ▲ +2
High 32 ▼ -5
Medium 15 ▼ -7
Low 45 ▲ +12

Budget utilization for cybersecurity initiatives 75% ▲ +22
Forecast for complete coverage 123% ▲ +7

February 2024
Ongoing tests 56
Assets 10
16%
46
12%
11%

Name	Start date	Status	Components nr.	Regulation	Risk level	Findings
Start		Ongoing	1	pci_dss tiber_ro	Critical	0

Zepo.

SIMPLIFYING AND AUTOMATING CRA COMPLIANCE

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA

February 2024

Antonio Muñoz - antonio.munoz@zepoapp.com

Deck Prepared for ECCC info Day Event: CYBERSECURITY DIGITAL EUROPE PROGRAM

At Zepo we are experts in the development of cutting edge technology, accessible and user friendly, to empower European SMEs with the knowledge and resources to remain compliant with regulation as well as aware of the existing risks in the cyber space.

Join us and let’s build together a tool to automate both penetration testing and training efforts to help SMEs be CRA compliant!

Z.

How can we contribute to the consortium?

Training material

- We are experts in the **development of training material**, specifically targeted for SMEs
- Our **learning methodology** includes a unique ***learning by doing*** approach that strengthens the effectiveness of the training purpose
- We are specialists in **digesting regulations** and making these **accessible for SMEs**

Technology automation (e.g., pentesting)

- We build **automated compliance tools** to guarantee alignment with

Experience with European SMEs

- We work **closely with European SMEs** and understand what it takes to be **successful in the dissemination of technology** and training material
- We have **global partnerships** in place that can help us **accelerate the dissemination** of our work to ensure an efficient CRA compliance

Status of our consortium and what capabilities or types of partners we are looking for.

Status

- We **haven’t identified any parties yet** and therefore are **interested in joining** an existing one or start one from scratch

Key parties that can complement the consortium

- Solid understanding of the **CRA compliance and requirements**
- Experience **validating and evaluating training** material content
- **Introduction to key parties**:
    - Network of National Coordination Centres (NCCs)
    - European Digital Innovation Hubs (EDIHs)
    - Relevant European and National cybersecurity entities

Expertise in drafting successful proposals

- Experience **managing (i.e., drafting and submitting)** European proposals
- Experience **coordinating and leading** consortiums in similar programs

Cyber Cert Labs

Bucharest, February 22nd 2024

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA

Patricia Shields, CEO, Cyber Cert Labs

cybercertlabs.com

Our Proposal

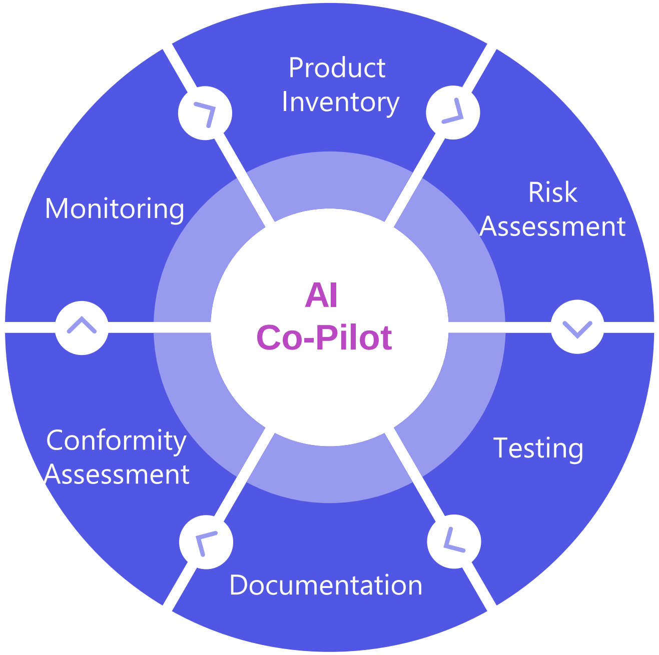
- To cover the entire CRA lifecycle
- Address the problem statements for SMEs and Micro SMEs – Complexity, Cost, Assurance, Knowledge and Skills gaps.
- A workflow engine with built-in AI Co-Pilot to automate the journey to compliance for SMEs.
- Integrate with other platforms to provide services such as pen testing on demand, vulnerability management, secure coding, consultancy and prepare for conformity assessment.
- Produce the necessary documentation such as SBOM, risk assessment results, vulnerability reports, secure coding outputs and declaration of conformity.
- Disseminate information and educate the market – Phase 1 - Readiness Assessment Questionnaire prototype demo …

Cyber Cert Labs

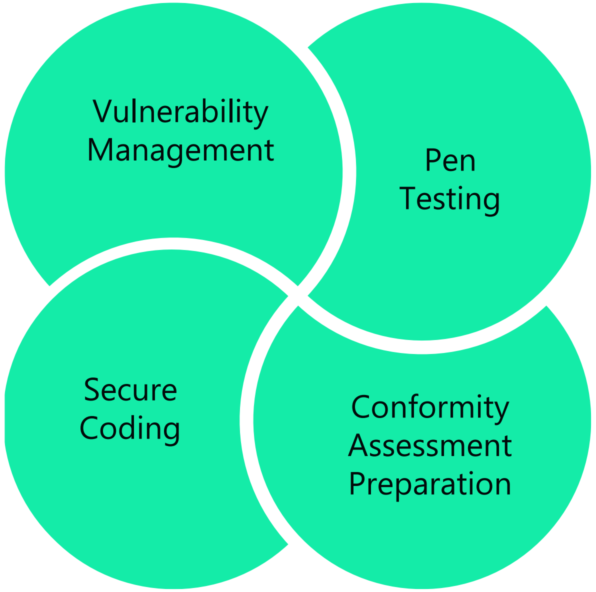
Our Mission

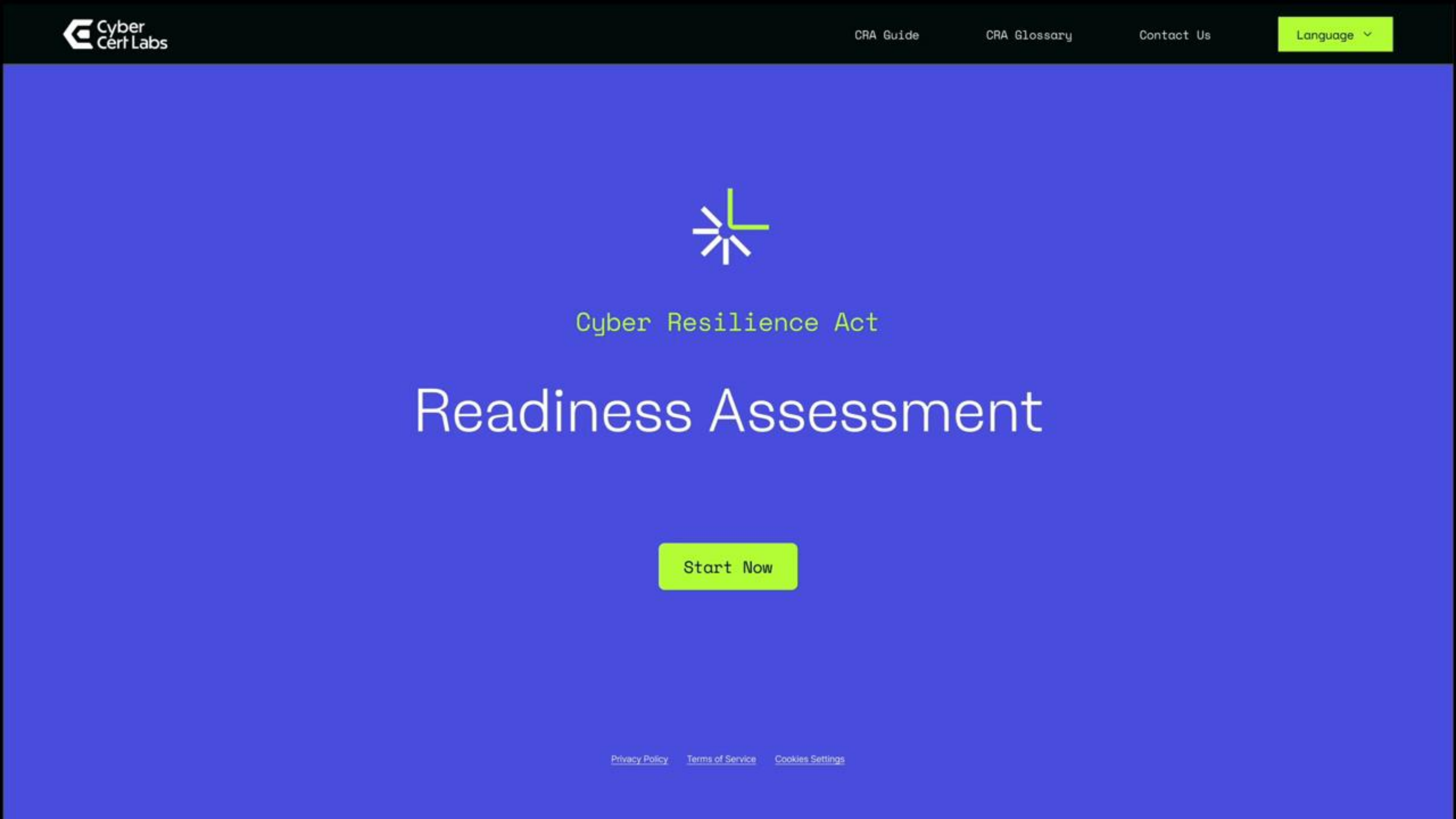
To build AI enabled software to guide SMEs and Micro SMEs through every step of their journey to achieve compliance with the Cyber Resilience Act. Supporting them from the initial product development stage right through to affixing the CE mark and placing their products on the market.

AI Workflow Engine



API Integrations





Cyber Resilience Act

Readiness Assessment

Our Consortium So Far …

	REFRACTED security	Protostars.ai	NRD Cyber Security	TBD
Cyber Cert Labs	Refracted	Protostars.ai	NRD	CAB - LAB
Ireland	Belgium	Ireland	Latvia	EU
Consortium Lead CRA Compliance Platform	Vulnerability Management Platform	AI Driven Secure Coding Analysis Platform	Test Customer	TBD

Cyber Cert Labs

Dogpatch Labs, CHQ Building, Custom
House Quay, North Dock, Dublin,
Ireland

Contact

Patricia Shields
Chief Executive Officer

Mobile: +353 833608039
Email: patricia@cybercertlabs.com

cybercertlabs.com

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY
Deployment of Post Quantum Cryptography in systems in industrial sectors

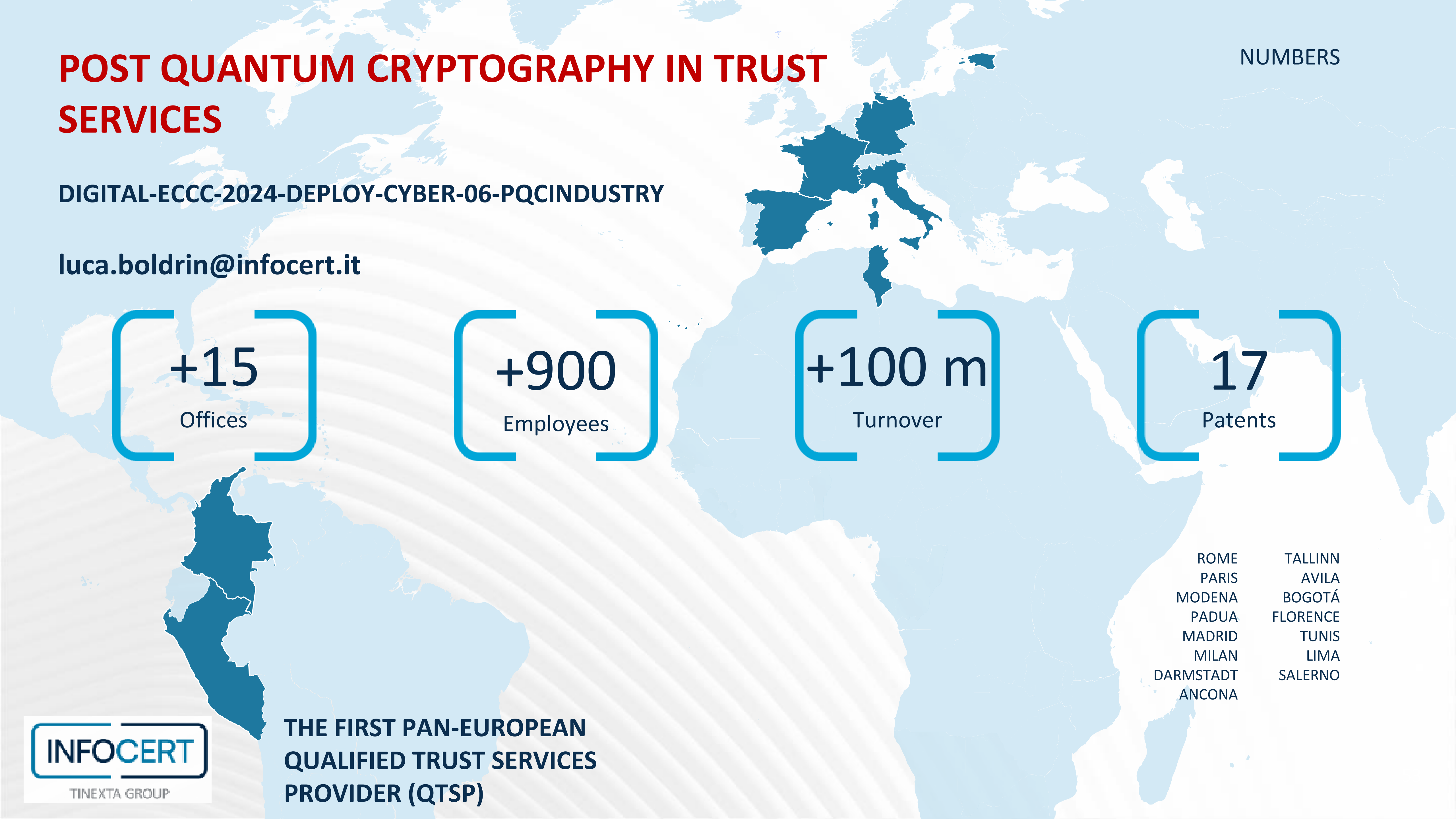
#	ORGANISATION	PRESENTER
1	infocert	Luca Boldrin
2	NoID Solutions Ltd	Rob Jones

POST QUANTUM CRYPTOGRAPHY IN TRUST SERVICES

NUMBERS

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY

luca.boldrin@infocert.it



+15
Offices

+900
Employees

+100 m
Turnover

17
Patents

ROME
PARIS
MODENA
PADUA
MADRID
MILAN
DARMSTADT
ANCONA

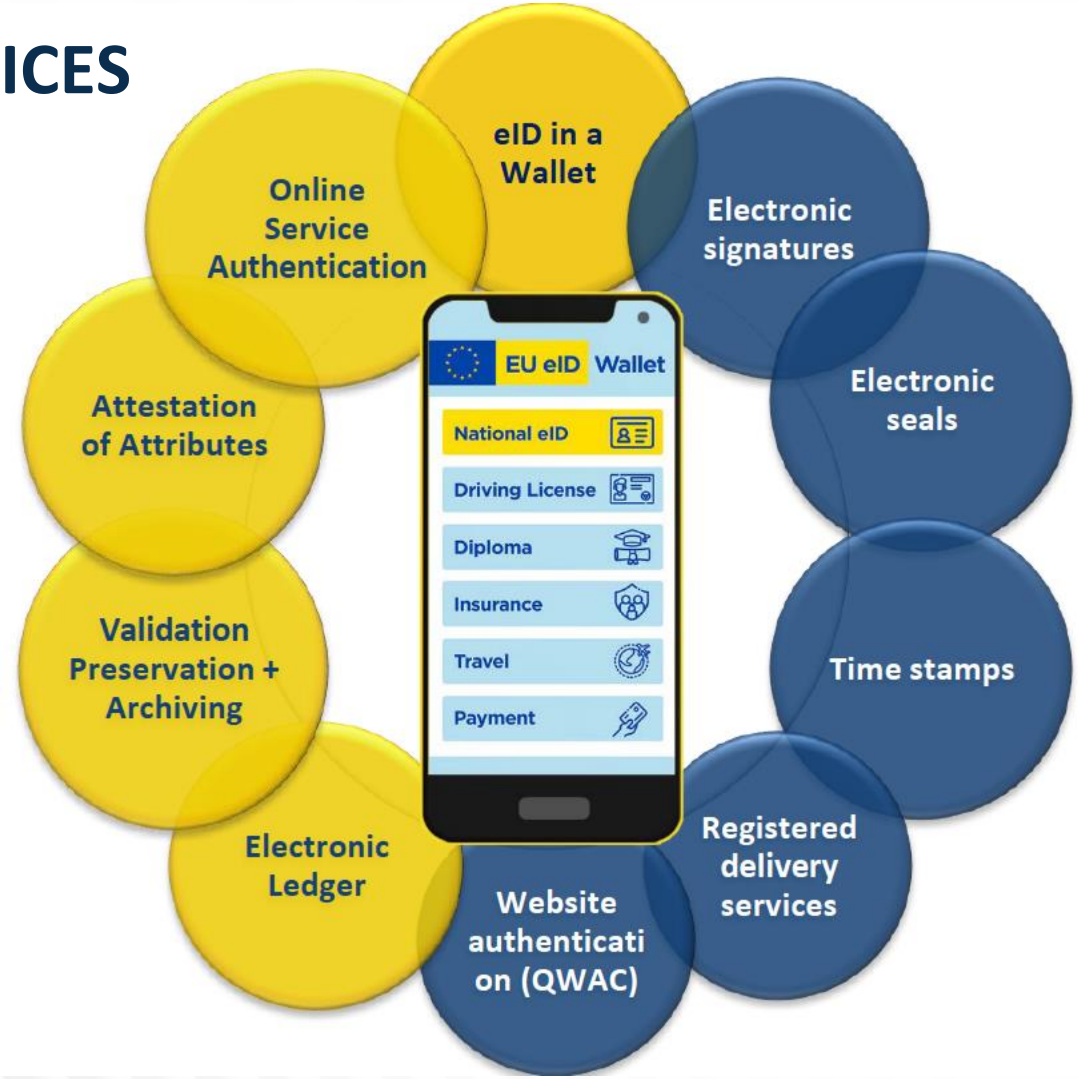
TALLINN
AVILA
BOGOTÁ
FLORENCE
TUNIS
LIMA
SALERNO

INFOCERT
TINEXTA GROUP

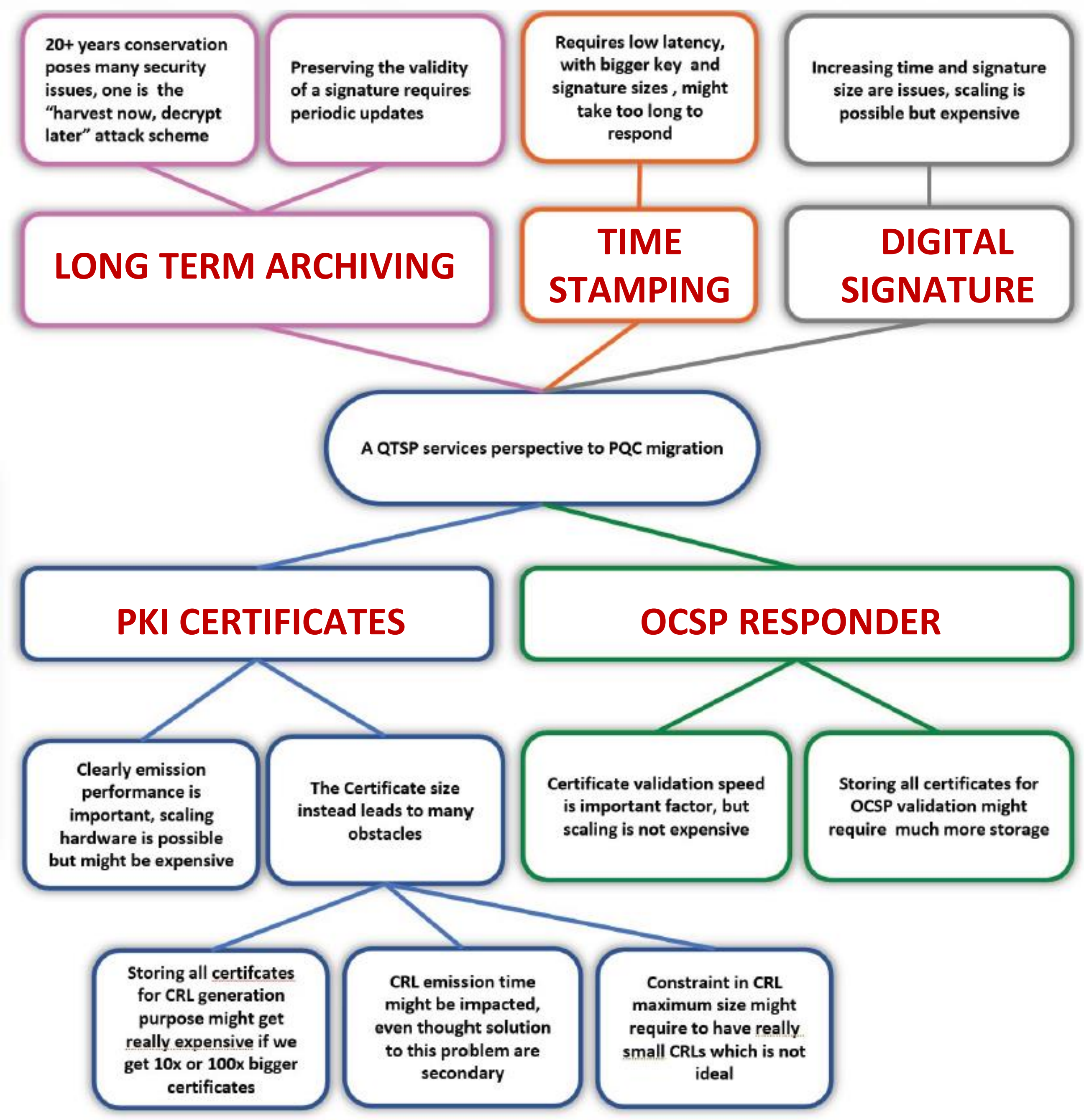
THE FIRST PAN-EUROPEAN QUALIFIED TRUST SERVICES PROVIDER (QTSP)

QSC STANDARDIZATION → TRUST SERVICES

Stakeholders		
3GPP (incl. SA2, SA3)		
ITS		
OneM2M		
ETSI TC ESI		
ETSI ISG PDL		
ISO/TC 307/JWG 4, WG6		
ITU-T Q. 14		
Global Platform		
LINUX Foundation		



TRUST SERVICES: ISSUES TO BE DEALT WITH



20+ years conservation poses many security issues, one is the "harvest now, decrypt later" attack scheme

Preserving the validity of a signature requires periodic updates

Requires low latency, with bigger key and signature sizes , might take too long to respond

Increasing time and signature size are issues, scaling is possible but expensive

LONG TERM ARCHIVING

TIME STAMPING

DIGITAL SIGNATURE

A QTSP services perspective to PQC migration

PKI CERTIFICATES

OCSP RESPONDER

Clearly emission performance is important, scaling hardware is possible but might be expensive

The Certificate size instead leads to many obstacles

Certificate validation speed is important factor, but scaling is not expensive

Storing all certificates for OCSP validation might require much more storage

Storing all certifcates for CRL generation purpose might get really expensive if we get 10x or 100x bigger certificates

CRL emission time might be impacted, even thought solution to this problem are secondary

Constraint in CRL maximum size might require to have really small CRLs which is not ideal

INFOCERT
TINEXTA GROUP

STATEMENT OF INTEREST:

Not part of a consortium yet – looking to join as a partner in a consortium in the role of:

1- implementing QSC standards applied to TRUST SERVICES in X-509 certificate issuance and document signing (CAdES, XAdES, PAdES, JAdES)

2- Pilot applicability (size, performance, latency) in specific scenarios (e.g. bank onboarding remote contract signing, long term document preservation)

INFOCERT

TINEXTA GROUP

THANK YOU

SIXTEMA
TINEXTA GROUP

Camerfirma
AN INFOCERT COMPANY

CERTEUROPE
AN INFOCERT COMPANY

ICTECHLAB
AN INFOCERT COMPANY

infocert.it infocert.digital

A presentation by Rob Jones, founder & CEO, NoID Solutions Ltd

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCINDUSTRY

Deployment of Post Quantum Cryptography in systems in industrial sectors

NoID develop and license email server software IP

We protect email and privacy, integrate it with chat, and

prevent bad things from happening

by blocking the major causes of cybercrime

Who and What are NoID?

Who we are

- a multi-national team with over 100 years of combined global business experience
- building software and internet infrastructure IP in the EU
- a cybersecurity startup based in Malta and a member of its NCC
- graduates of the prestigious Silicon Valley based accelerator PLUGANDPLAY

Our vision, our mission

To become the de-facto choice for secure email and chat in organizations large and small. Be recognized for delivering privacy, reducing risk and improving the environmental footprint of email.

Important

We are already building a post quantum ready email server platform. This funding will assist with our mission, we are not dependent on it.

The Problem

Today

90% of cybercrime involves email

10’s of billions of **$ £ € ¥** are lost by business and consumers every year

globally **300 billion** emails are sent daily

99% of all email is not encrypted when it travels or when it is at rest

Existing POP3/IMAP/SMTP/Email encryption

- uses “HTTPS / TLS” which is not post quantum compliant
- existing “end-to-end” methods require manual configuration. They may or may not be compliant
- is “bespoke” to a domain and not interoperable between domains without manual intervention

50 year old email is “not fit for purpose“ in the 2020’s or regarding Post Quantum readiness

The Solution

Post Quantum world

Server to server SMTP is replaced with a non-proprietary Post Quantum compliant method (**PQTP**)

- Release a new PQC cross-platform method of exchanging email “freely” available to all server software providers
  - Email sent to non-PQ compliant servers will be delivered as usual to prevent chaos
  - Receiving compliant servers change to a new “PQ handshake and exchange method”

Partners and our route to market

We are working with Microsoft, AWS, Internet Service Providers, Cloud Technology providers, Consultants and Cybersecurity businesses located in USA, France, Germany, Malta, UK and elsewhere. We build the IP, others deliver it to customers.

Maximizing communication is vital. If you can help we would love to hear from you. The entire cybersecurity and technology community must be involved.

Reach out via https://noid.ltd, linkedin or rj@noid.ltd. Thank you, any questions?

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC
Standardisation and awareness of the European transition to postquantum cryptography

#	ORGANISATION	PRESENTER
1	ABI Lab	Mario Trinchera

ABI Lab

ABI Lab

ABI Lab is the Research and Innovation Centre promoted by the Italian Banking Association that provides thought leadership in banking and financial services.

Our primary purpose is to foster collaboration between banks and ICT companies on innovative technology to strengthen the efficiency of financial services.

Through its Centres of Excellence, ABI Lab conducts primary research in critical areas including Digital Transformation, Fintech, Blockchain/DLT, Cybersecurity, AI, IT and operations, and Sustainable Transition.

ABI Lab also manages the activities of **CERTFin, Computer Emergency Response Team for the Italian Financial Sector**, a public-private partnership chaired jointly by Bank of Italy and Italian Banking Association (ABI).

CERTFin aims to enhance cyber risk management capabilities among financial operators and bolster the cyber resilience of the Italian financial sector through operational and strategic support activities focused on prevention, preparation, and response to cyber attacks and security incidents.

.

KEY FACTS

2002
ABI Lab foundation

7
Expertise Centres

120
Banks

15
Annual research reports

20
Working groups

69
Companies

A Methodology for the Financial Sector

Our proposal is to create a methodology specific to the banking sector that fully supports, from an operational and strategic point of view, all actors involved in the migration process, particularly payment systems, towards quantum-resistant algorithms.

Thus, migration to quantum-resistant algorithms is a preventive step to ensure that information security systems remain robust and reliable even when QC becomes a practical and scalable reality. Incidentally, as a structured migration process takes time, it is prudent to start the process early to avoid future risk exposure.

An exhaustive migration process cannot but begin by **identifying all instances** of the use of public key algorithms in hardware, network infrastructure, operating systems, application programmes, communication protocols, PKIs, and access control mechanisms.

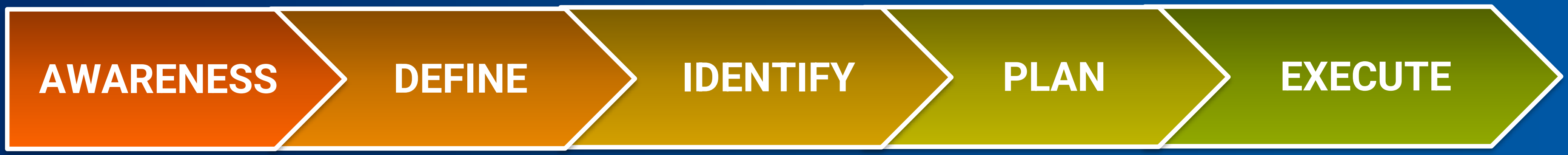
Once the affected assets have been identified, it will be necessary to **prioritise** the components that must be considered first in the migration as they are considered to be at higher risk.

Systematic approaches should be adopted to migrate from vulnerable to quantum-resistant algorithms among the different types of assets, **ensuring to verify compatibility with the underlying support technology.**

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD

Migration Process

We can identify **five macro-phases** of a hypothetical migration plan:



Quantifying the time needed to move from one phase to the next is impossible. The awareness phase takes a long time; at this stage, it should already be finished to proceed with the subsequent phases. However, we know that the sensitivity to these issues is still very low.

Some US government agencies, such as the NSA, have already stated that they can only complete the migration after ten years; it is hard to imagine that it will be better in Europe.

We are looking for partners interested in contributing to this methodology

✉ **mario.trinchera@certfin.it**

The Stages

- **Awareness**: This phase aims to align management by making them understand the risks associated with delayed issue management.
- **Define** (or Preparation): This phase focuses on defining objectives strategy, building a roadmap, estimating the necessary budget, setting up the working group, etc. It is essential to concentrate expectations on the short, medium, and long-term.
- **Identify** (or Discovery): To identify all the areas where encryption algorithms are used (sw, hw, and services) internally within the company and by third parties. The primary aim is to build a searchable ***crypto-inventory*** that is kept up-to-date and makes it possible to identify where to intervene and with what impact if a used encryption methodology needs to be replaced.
- **Plan**: In this phase, interventions are planned in line with a 'Quantum Threat Model' to prioritize interventions. It is essential to focus on the lifespan of the data (e.g., it may not be necessary to protect a contract that lasts one year).
- **Execute**: Activities that may range from hybrid logic to entirely post-quantum logic. One aspect to be prioritized is ***agile crypto management***, starting with the governance of cryptographic material.

Session Agenda

Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-TRANSITIONEUPQC
Roadmap for the transition of European public administrations to a post-quantum cryptography era

#	ORGANISATION	PRESENTER
1	University Politehnica of Bucharest	Bogdan-Calin Ciobanu

Quantum @ UPB

ECCC Info Day

Bogdan CIOBANU

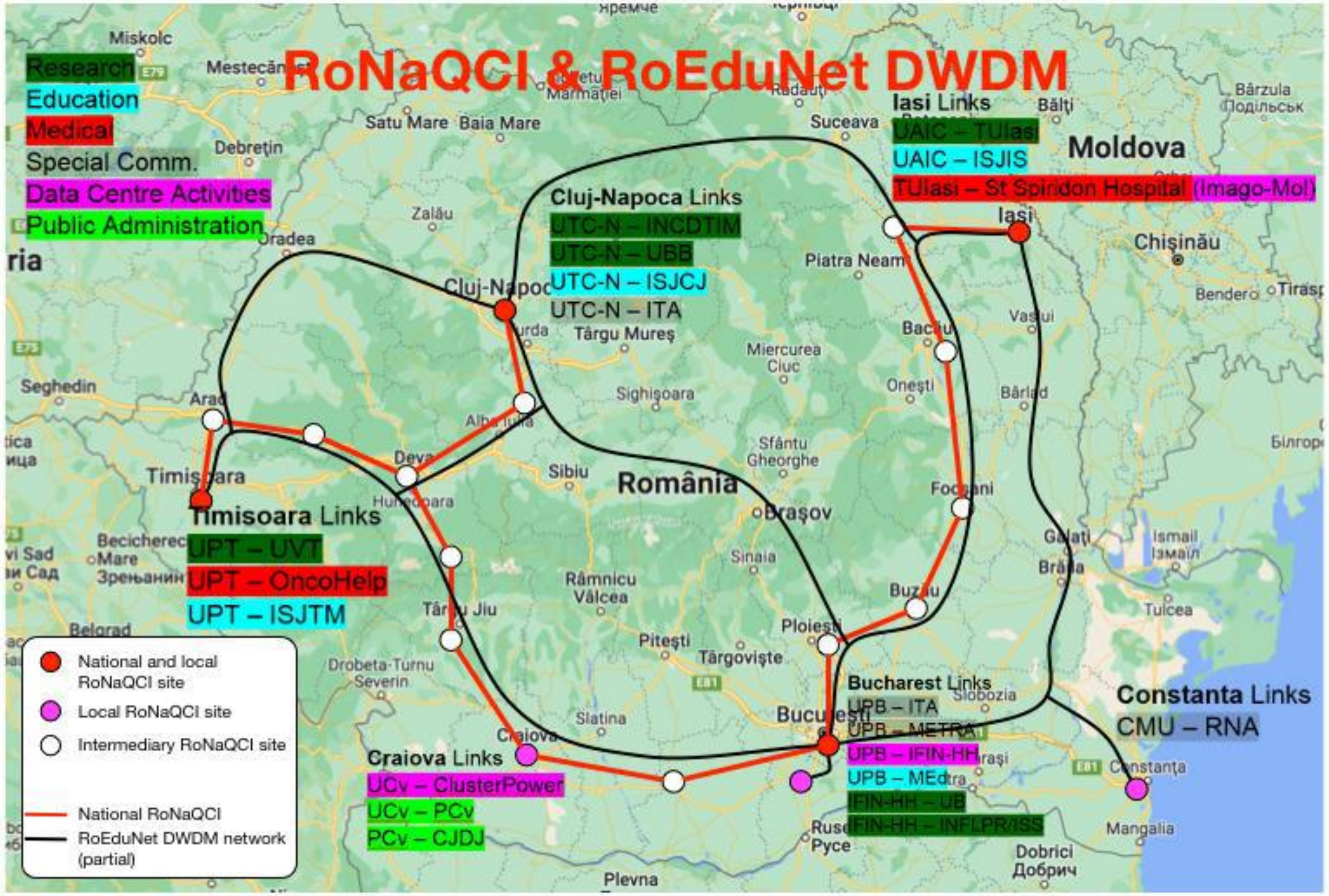
University POLITEHNICA of Bucharest
Quantum Laboratory

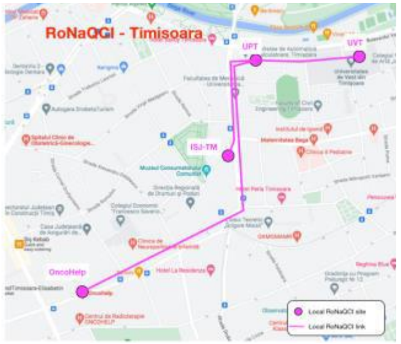
22 February 2024

quantum.upb.ro

Quantum @ UPB – UPB coordinates RoNaQCI

Romanian **Na**tional **Q**uantum **C**ommunication **I**nfrastructure, the largest terrestrial QKD network from EU as part of EuroQCI.

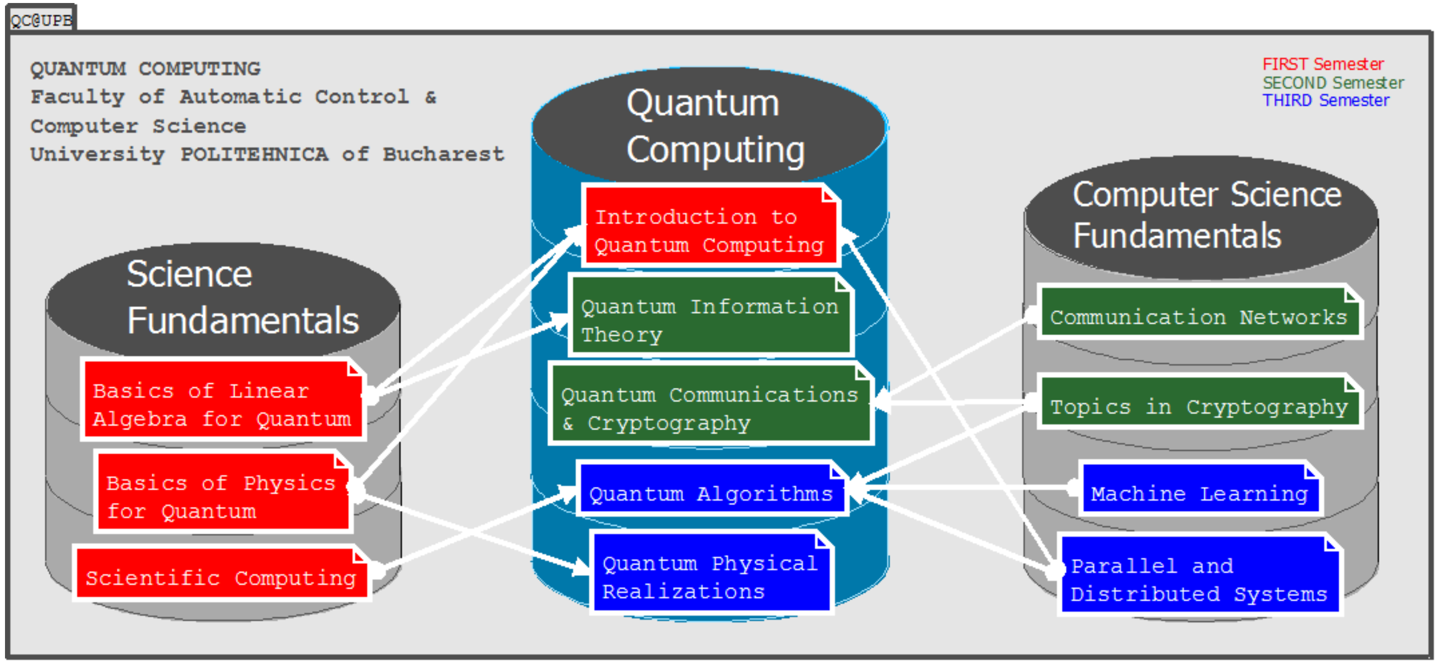




Quantum @ UPB - Education

UPB started the **Quantum Computing MSc.**, the first master program quantum related from RO, lead by prof. PGPopescu.

"I think I can safely say that nobody understands Quantum Mechanics"
RICHARD FEYNMAN
"Spooky action at a distance"
ALBERT EINSTEIN
"Not only is the Universe stranger than we think, it is stranger than we can think"
WERNER HEISENBERG
uantum
FACULTATEA DE AUTOMATICA SI CALCULATOARE
@UPB
quantum.upb.ro
First Quantum MSc in Romania
Third Quantum Computing MSc in EU*
Grand Opening
QUANTUM COMPUTING
14 Nov 2023
FROM 17:00 IN EF00?
|0⟩
|0⟩
|0⟩
|0⟩
H
X
H
H
H
H
H
?
(base2)
*to our knowledge



QUANTUM COMPUTING
Faculty of Automatic Control & Computer Science
University POLITEHNICA of Bucharest

Science Fundamentals
- Basics of Linear Algebra for Quantum
- Basics of Physics for Quantum
- Scientific Computing

Quantum Computing
- Introduction to Quantum Computing
- Quantum Information Theory
- Quantum Communications & Cryptography
- Quantum Algorithms
- Quantum Physical Realizations

Computer Science Fundamentals
- Communication Networks
- Topics in Cryptography
- Machine Learning
- Parallel and Distributed Systems

Pantelimon George Popescu este profesor dr. ing. la Departamentul de Calculatoare, Facultatea de Automatică și Calculatoare, UPB, fiind titular [illegible] cursurilor: Metode Numerice și Introducere în Quantum Computing. Domeniile sale de interes științific acoperă Quantum Computing, Information, Teoria Informației, Analiză Numerică [illegible]egalități.

Octavian Stănășilă este profesor [illegible] la Facultatea de Automatică și [illegible] UPB, specialist în Analiză [illegible] aplicate (Matematică [illegible] schimburilor de căldură [illegible] 100 de lucrări și monografii [illegible] premiul Academiei Române [illegible] Secția Informatică.

978-606-515-[illegible]

editura POLITEHNICA PRESS

P.G.Popescu O.Stănășilă

PROVOCĂRILE CALCULULUI CUANTIC

PROVOCĂRILE CALCULULUI CUANTIC

Carte de învățătură

Pantelimon George Popescu Octavian Stănășilă

uantum

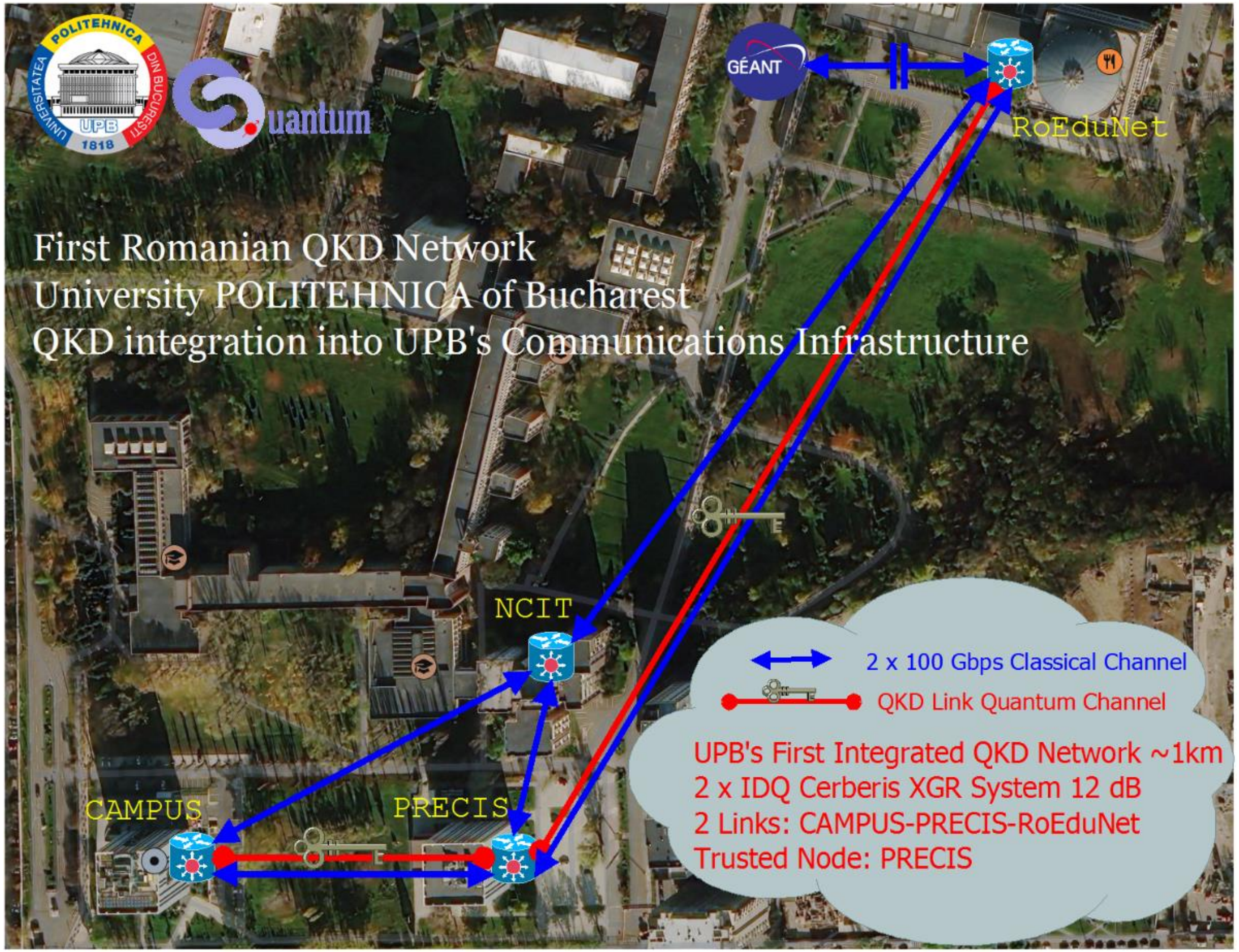
uantum

IBM Bitdefender certSIGN dexonline

UNIVERSITY POLITEHNICA OF BUCHAREST 205 YEARS OF INNOVATION QUANTUM

Quantum @ UPB – First RO QKD Network

QKD net. integrated into UPB's Communication Infrastructure.



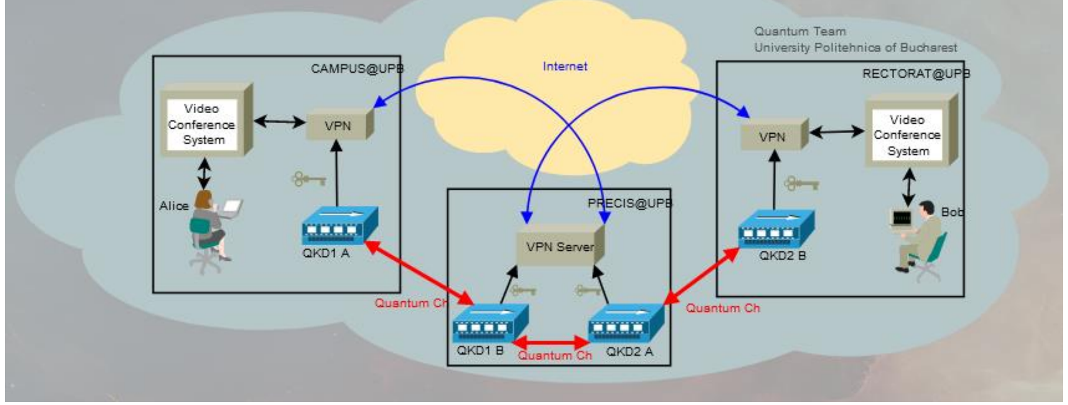
First Romanian QKD Network
University POLITEHNICA of Bucharest
QKD integration into UPB's Communications Infrastructure

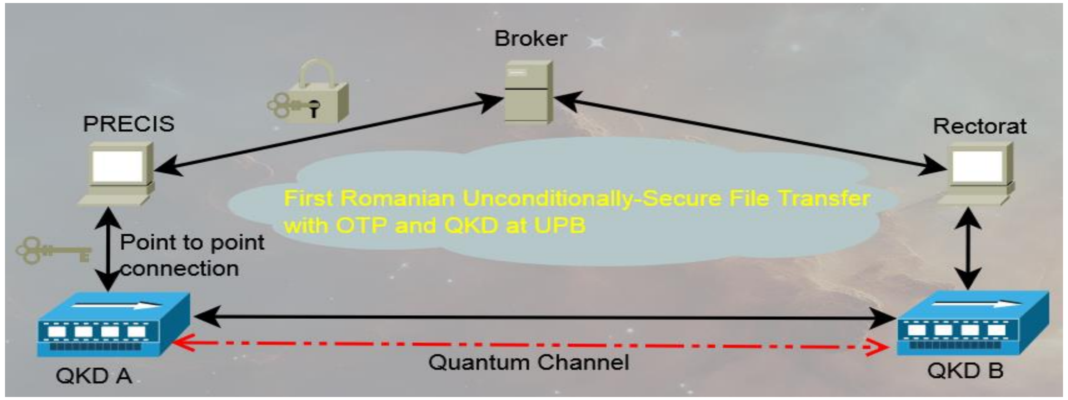
2 x 100 Gbps Classical Channel

QKD Link Quantum Channel

UPB's First Integrated QKD Network ~1km
2 x IDQ Cerberis XGR System 12 dB
2 Links: CAMPUS-PRECIS-RoEduNet
Trusted Node: PRECIS

First video conference over a post-quantum VPN from Romania, enhanced by QKD





First Romanian Unconditionally-Secure File Transfer with OTP and QKD at UPB

Thank you!

quantum.upb.ro

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.