CS SESSION - MODERATORS

Roberto Cascella
roberto.cascella@ecs-org.eu

Salvatore D'Antonio
salvatore.dantonio@uniparthenope.it

Branka Stojanovic
branka.stojanovic@joanneum.at

CS Review Team:
Roberto Cascella | Salvatore D'Antonio | Branka Stojanovic

CS-01-01 - 8
CS-01-02 - 4
CS-01-03 - 3
CS-01-05 - 1
CS-01-06 - 1

CS SESSION - PRESENTATIONS

CS-01-01	***Ivo Häring***	*ivo.haering@emi.fraunhofer.de*
	Graziano Giorgi	*graziano.giorgi@zanasi-alessandro.eu*
	Tatiana Silva	*tatiana.silva@treetk.com*
	Inés Ortega Fernández	*iortega@gradiant.org*
	Marco Tiemann	*marco.Tiemann@innovaintegra.com*
	Aitor Corchero	*aitor.corchero@eurecat.org*
	Mojmír Mamojka	*mojmir.mamojka@akademiapz.sk*
	Gizem Bozdemir	*gizem.bozdemir@pal-robotics.com*

CS-01-02	***Jordi Herrera-Joancomartí***	*jordi.herrera@uab.cat*
	Raúl Orduna-Urrutia	*rorduna@vicomtech.org*
	Rita Nogueira	*rita.nogueira@treetk.com*
	Mario Pichler	*mario.pichler@scch.at*

CS SESSION - PRESENTATIONS

CS-01-03	***Petr Dzurenda***	*dzurenda@vut.cz*
	Cristina Pérez-Solà	*cristina.perez@uab.cat*
	Aitor Corchero	*aitor.corchero@eurecat.org*
CS-01-05	***Aitor Corchero***	*aitor.corchero@eurecat.org*
CS-01-06	***Sara Ricci***	*ricci@vut.cz*

CS-01-01

HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications

Presenters
CS-01-01:

Ivo Häring	*ivo.haering@emi.fraunhofer.de*
Graziano Giorgi	*graziano.giorgi@zanasi-alessandro.eu*
Tatiana Silva	*tatiana.silva@treetk.com*
Inés Ortega Fernández	*iortega@gradiant.org*
Marco Tiemann	*marco.Tiemann@innovaintegra.com*
Aitor Corchero	*aitor.corchero@eurecat.org*
Mojmír Mamojka	*mojmir.mamojka@akademiapz.sk*
Gizem Bozdemir	*gizem.bozdemir@pal-robotics.com*

GRAICE: Generative AI for Resilient and Automated Intelligent Cybersecurity and Compliance Evaluation

- ***Lola De-Acuña***; *Ivo Häring*
- ***macuna@us.es***; *ivo.haering@emi.fraunhofer.de*
- ***University of Sevilla***; *Fraunhofer EMI*

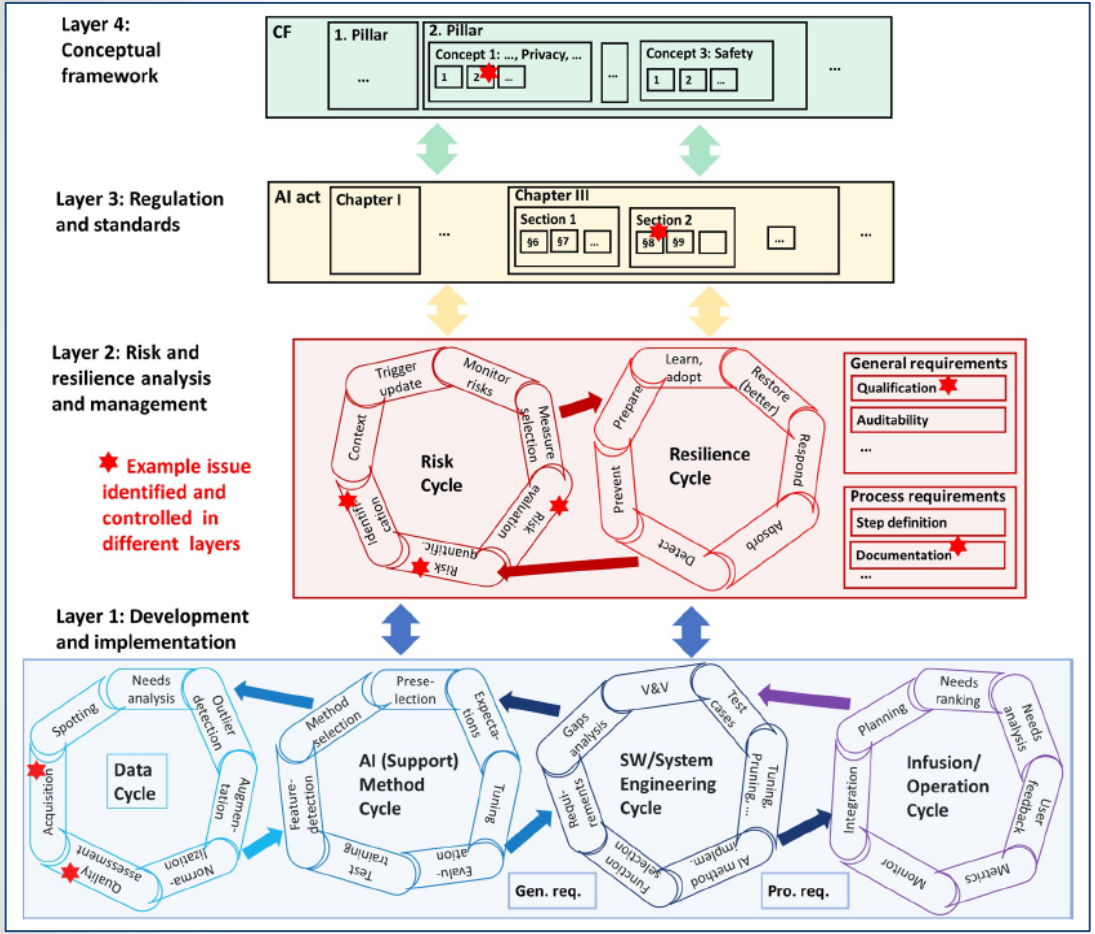
- **Roles:** ***Coordinator***; *Support technical-scientific coordination*

- Topic to be addressed: CL3-CS-01

Proposal idea/content

- Layered Framework for the safety and security assessment of AI-based systems.
- Simulation and virtual cyber resilience testing, also live.
- Coverage of AI/Cyber resilience act, NIS2 and General Data Protection Regulation (GDPR).
- Supporting complex risk analysis in systems and critical infrastructures and using AI to detect critical events and recommend actions.
  - **E.g. Based on Cross Impact Analysis (CIA), Interpretative Structural Modeling (ISM) algorithms, and predictive fast engineering network simulation, causal network analysis and inference.**

Lola De-Acuña, macuna@us.es; Ivo Häring, Ivo.Haering@emi.fraunhofer.de



- **Layered framework for Cyber Security Management and quantitative compliance assessment.**
- **Approaches are applied to Development and Operation cycle and steps**
- **Application to use cases**

Towards an Automatable Framework for Compliance Assessment of AI-Based Systems Through Early Risk Detection and Management in the Health Sector

Ivo Häring[1], Gaia Bondani[2], Francesca Lonetti[3], Rebeca Gutiérrez[4], Julián A. García-García[5], Nicolás Sánchez-Gómez[5], Guglielmo De Angelis[6], and Lola De-Acuña[5]

Project participants

- Existing consortium:
  - Proposed coordinator: University of Seville (Spain)
  - Partners / Other participants:

Type	Country (nº)	Status
University	Germany (1), Italy (3), UK (1), Greece(1)	Confirmed
Research centre	Spain (2), Germany (1), Italy (1)	Confirmed
Industry	Spain (2), Italy (2)	TBC
SME	Spain (2), Greece(1), Cyprus (1)	TBC
Medical centre	Spain (1), Italy (1), Greece (1)	Confirmed

- Looking for partners with the following expertise/ technology/ application field:
  - **Companies with operational applications of AI for cybersecurity and/or compliance, particularly for EU Critical Infrastructure Networks.**
  - **National authorities, certification organisations, and bodies.**

SMI2G
Security Mission Information & Innovation Group

SAMURAI

Smart **A**utonomous **M**echanism for **U**nmasking,
Responding and **A**nalyzing **I**ntrusions

CL3-2025-02-CS-01
Option (a)

Graziano Giorgi

Zanasi & Partners
Security Research and Advisory

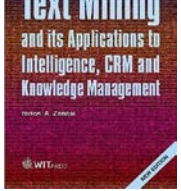
Zanasi & Partners

Strong expertise in **cybersecurity/cyberdefence:**

- Cybersecurity responsible in **P101** *(Protection of CBRN critical infrastructures in Europe, Middle East and Central Asia)*
- WP leader in **ACTING** *(Advanced European platform and network of Cybersecurity training and exercises centres)*

Strong expertise in **Artificial Intelligence**:

- Scientific Coordinator of **NEMO** *(HLT for Defence)*
- 30+ years of experience in **AI** and **Text Mining**:
  - Carabinieri Scientific Investigation Centre in Rome (IT)
  - IBM Research in Paris (FR) and San José (USA)
  - TEMIS (FR, IT, DE, USA)
  - Universities of Bologna (IT) and Paris (FR)



Graziano Giorgi (graziano.giorgi@zanasi-alessandro.eu)

Proposal idea

Realise an **AI-driven deception system** to attract attackers into fake but realistic, dynamic environments.

- **GenAI** (e.g. LLMs) to create a «script» of a verisimilar, vulnerable environment (hosts, traffic, etc.)

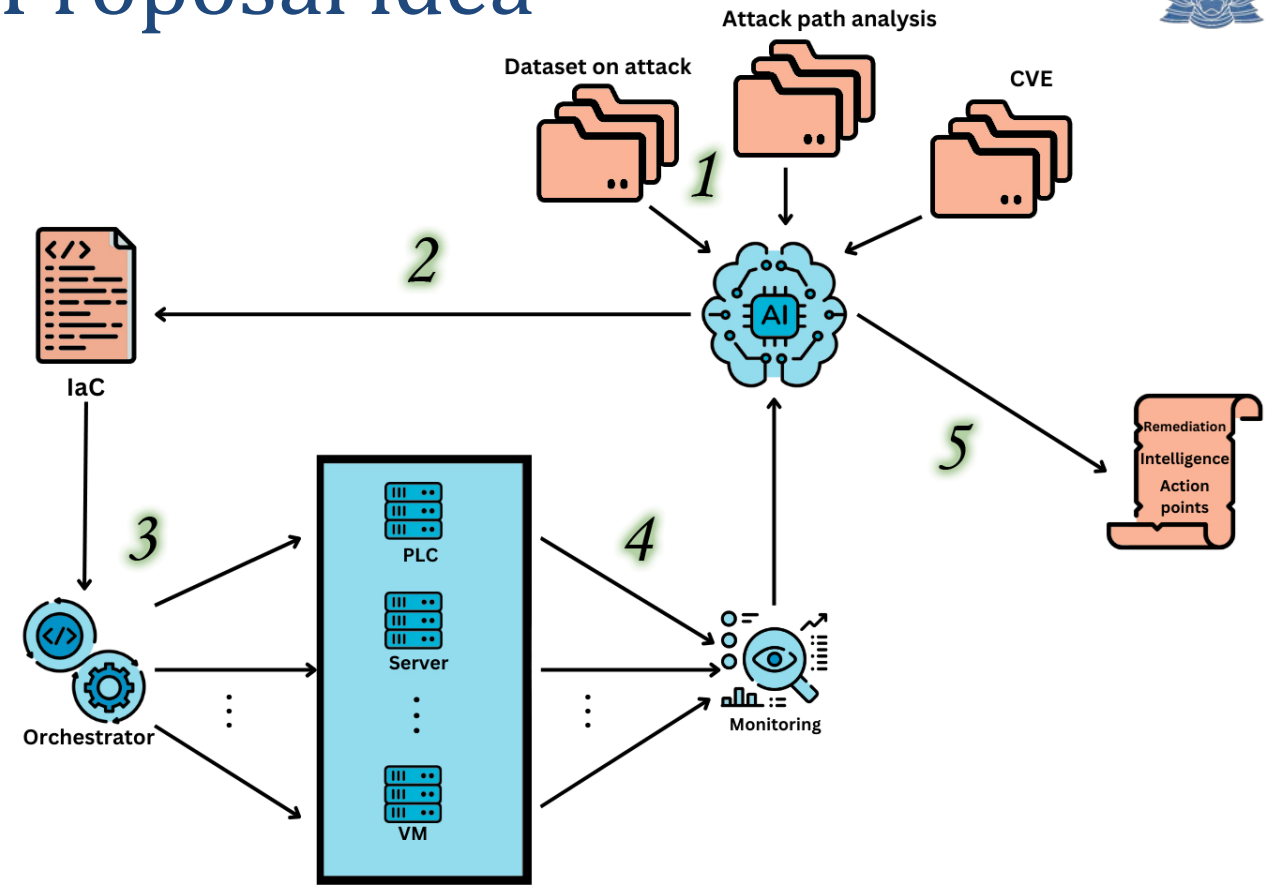
- **Infrastructure as Code** (e.g. Terraform) to automatically «put in place» the environment, waiting for attackers

- **Monitoring** the attackers behaviour on the known vulnerabilities of the fake attack surface

- Provision of **remediations** to protect real assets

Graziano Giorgi (*graziano.giorgi@zanasi-alessandro.eu*)

Proposal idea



Graziano Giorgi (graziano.giorgi@zanasi-alessandro.eu)

Project participants

- **Consortium**:
  - Zanasi & Partners [IT]: Scientifical coordinator or WP leader
  - 1 research institute [FR]
  - 1 cybersecurity legal expert [IT]
  - 2 critical infrastructure stakeholders [Eastern Europe]

- **Looking for** experts in:
  - Generative AI
  - Infrastructure as Code
  - OT cybersecurity
  - System integration

- **Z&P is also interested in:**
  - *CS-02*
  - *CS-03*
  - *DRS-01*
  - *DRS-02*
  - *DRS-03*
  - *BM-01*

Graziano Giorgi (*graziano.giorgi@zanasi-alessandro.eu*)

- *Tatiana Silva*
  - *tatiana.silva@treetk.com*
- *TREE TECHNOLOGY (Spanish SME)*

  - *Participation in > 30 EU projects*
  - ***10 on-going H2020/HEUR projects***
  - *Expertise in* ***Big Data, AI, Computer Vision,*** *and* ***cybersecurity***

- Role: *S/T provider (WP leader)*
- Topic to be addressed: **HORIZON-CL3-2025-02-CS-01 Generative AI for cybersecurity applications**

GENIUS-SEC: Generative Intelligence for Unpredictable Security Threats

Option a. Developing, training and testing of Generative AI models for monitoring, detection, response and self-healing capabilities in digital processes, and systems against cyberattacks, including adversarial AI attacks.

Motivation

- Cyberattacks are evolving faster than ever — particularly zero-day threats and sophisticated, never-before-seen attack vectors.
- Current cybersecurity systems are reactive, slow to adapt, and heavily reliant on human intervention.
- Organizations face increasing downtime, data loss, and compliance risks due to the lack of autonomous, predictive defenses.

Solution

generative AI-based cybersecurity platform designed to:

- **Simulate attack scenarios** before they happen, in dynamic contexts.
- **Generate defensive responses** and recovery strategies in real-time, including zero-day.
- **Accelerate malware analysis** using AI-based reverse engineering.
- **Empower defenders**—both human and machine—with continuously updated threat intelligence and scenarios.

It is not just reactive security. It is **predictive, proactive, and self-healing**.

Tatiana Silva (tatiana.silva@treetk.com)

GENIUS-SEC: Generative Intelligence for Unpredictable Security Threats

Generative Threat Engine

AI Core Brain

Self-recovery module

AI-based Attack Simulator

Malware Reverse Engineering

Key Innovation Pillars

1. 🧠 **Generative Threat Engine** – Anticipates novel attack variants and suggests proactive defenses.
2. 🎯 **AI-based Attack Simulator** – Trains systems and people using realistic, unseen cyberattack scenarios.
3. 🔄 **Self-Recovery Module** – Automatically generates and executes tailored recovery plans post-incident.
4. 🧬 **Malware Reverse Engineering** – Speeds up response to new malware families using generative models.

All powered by **explainable AI** and optionally enhanced through **federated learning for privacy-preserving collaboration.**

Tatiana Silva (tatiana.silva@treetk.com)

Project participants

- Looking for partners with the following expertise:
  - Coordinator
  - Strategic partners in cybersecurity, threat intelligence
  - Expert in legal and ethics aspects, in particular knowledge in the use of generative AI in research, ethics for trustworthy AI
  - Technical partners who can complement this idea
- Tree Technology's role
  - WP leader
    - Generative AI
    - Attack simulation, detection and response
    - Malware analysis using AI: behavioural patterns

Tatiana Silva (tatiana.silva@treetk.com)

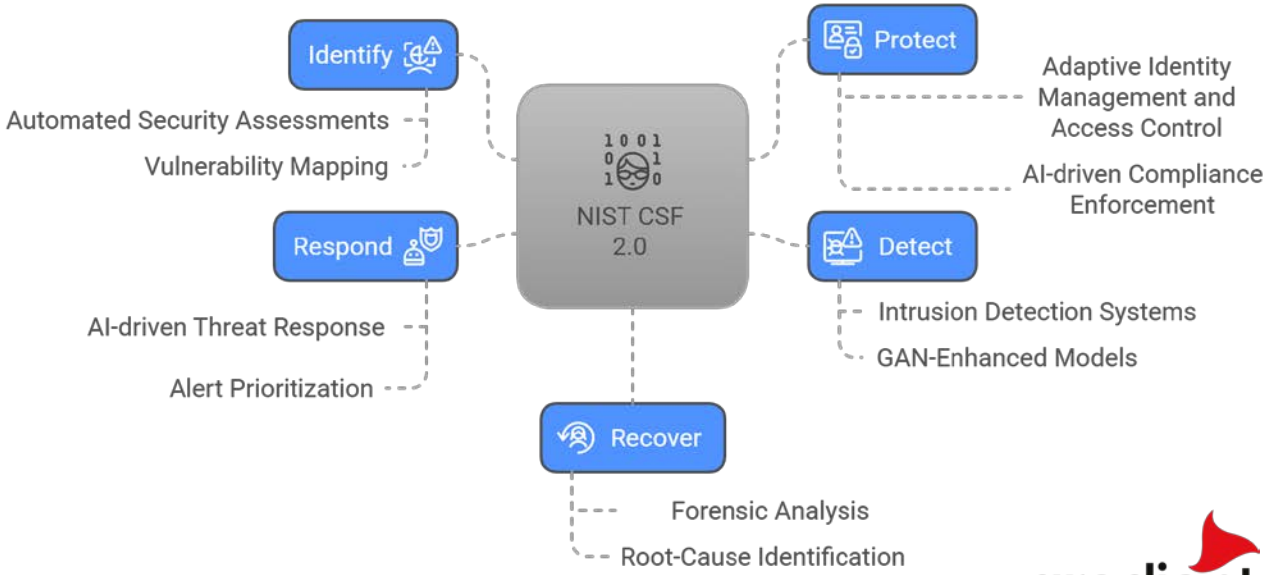
GENSEC: Generative AI for Next-Generation Cybersecurity

- *Inés Ortega Fernández*
- *iortega@gradiant.org*
- *Gradiant (RTO, Spain)*

- Role: *Proposal coordinator, WP Leader, S/T provider*

- Topic to be addressed: **CS-01 Generative AI for Cybersecurity applications**

Proposal idea/content



gradiant
Connectivity · Intelligence · Security
for your business

Inés Ortega Fernández / iortega@gradiant.org

Project participants

- **Existing consortium:**
  - Proposed coordinator: *Gradiant* - GenAI model development and fine-tuning, AI Agent Development, Anomaly Detection
  - Other partners: including Barcelona Supercomputing Center (AI + HPC infrastructure), Nuromedia (software development), University of Bari (AI Ethics & Governance).
- **Looking for partners** with the following capabilities:
  - *GenAI (GANs and adversarial resilience, AI-driven access control)*
  - *Threat Intelligence & Vulnerability Analysis*
  - *CTI providers with access to structured/unstructured cyber threat data.*
  - *Data Capture and analytics (deep web data crawling, MLOps, Big Data platform development).*
  - *Expertise in Digital Forensics*
  - *AI Governance and Regulatory Compliance*
  - *Demonstrator Builder (piloting and TRL elevation)*

gradiant
Connectivity · Intelligence · Security
for your business

Inés Ortega Fernández / iortega@gradiant.org

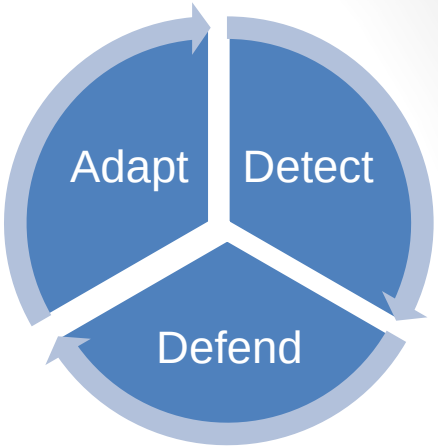
GenAI Sentinel

- *Marco Tiemann*
- *marco.Tiemann@innovaintegra.com*
- *Innova Integra (UK)*
- Role: *Proposal coordinator*

- Topic to be addressed:

CL3-2025-02-CS-01 a) (ii) Adaptive Security Measures

GenAI Sentinel



- *Research focus on adaptive GenAI security measures for cyber security:*
  - *GenAI for enhanced real-time threat detection*
  - *GenAI for automated threat defence*
  - *Automated threat data exchange for continual learning*
  - *Robustness of adaptive GenAI protection measures against GenAI attacks*
- *Application use cases under consideration:*
  - *Security of online services*
  - *Security of autonomous systems*
  - *Security of GenAI systems*

Marco Tiemann, marco.tiemann@innovaintegra.com

Project participants

- Existing consortium:
  - Proposed coordinator: *Innova Integra (UK)*
  - Partners / Other participants:
    - 2 Leading research university partners
    - 1 Large research institute
    - 1 Large cyber security consulting firm
    - 2 end user partners
- Looking for partners with the following expertise/ technology/ application field:
  - *Further research partners*
  - *Further industry partners with cyber security apps in the market*
  - *Further use cases and related partners*

Marco Tiemann, marco.tiemann@innovaintegra.com

Generative AI-Driven Resilience (GEN-AIRISE)

HORIZON-CL3-2025-02-CS-01: Generative AI for Cybersecurity applications

Aitor Corchero – Innovation Manager at IT&OT Security
[Ideas- WP Leader/Partner]

"innovating with businesses"

Our Contribution: GEN-AIRISE

The Challenge

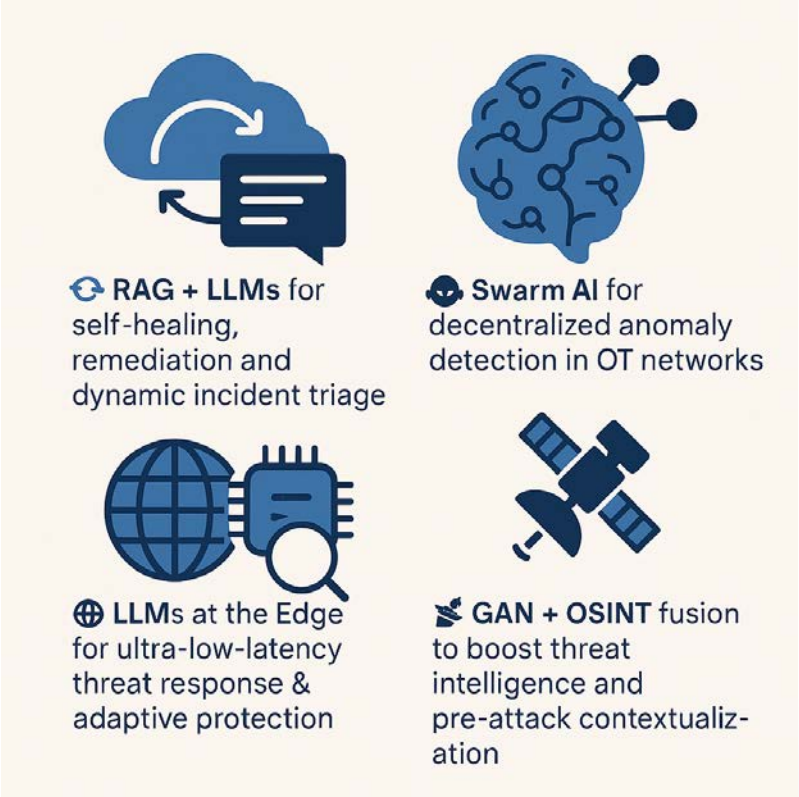
- Increasing AI-powered cyber threats in IT & OT infrastructures
- Static tools unable to adapt to new attacks
- Initial Levels of the SOC and incident centers specialists are required for complex attacks

Our Contribution: GEN-AIRISE

SMI2G
Security Mission Information & Innovation Group

Our Proposed Contribution

“A trustworthy, explainable and autonomous GenAI framework tailored to defend Europe’s IT/OT infrastructures from advanced cyber-physical threats.”



Join our Journey

- We bring an **experienced team** with proven Horizon track record
- Increase from TRL 4–6 GEN-AIRISE tested in EU projects like ATHENA and PLIADES
- Ready to integrate with your use cases and cross-border pilot scenarios

Let's lead the next wave of EU cybersecurity innovation together

Contact: Aitor Corchero
Eurecat | aitor.corchero@eurecat.org

Police Academy in Bratislava, Slovakia

- prof. JUDr. Mojmír Mamojka, PhD.
  Vice-rector for Science and Foreign Relations

- mojmir.mamojka@gmail.com
- mojmir.mamojka@akademiapz.sk

- Police Academy in Bratislava, Slovakia
  (the only university in Slovakia that operates as a departmental university under the Ministry of the Interior and is focused on „Security sciences" and the education of future police officers)

- Possible WP leader (consortium partner)

- HORIZON-CL3-2025-02-CS-01:
  ,,Generative AI for Cybersecurity applications“
  based on the Horizon Europe's Civil Security for Society 2025 Work Programme (early draft)

Proposal idea/content

Description of the proposed project:

- Developing, training and testing AI tools for law enforcement purposes with an emphasis on monitoring public profiles on social networks in an effort to prevent terrorist acts and detect other risks threatening public order

Key strong/selling points:

- Developing, training and testing AI tools
- Law enforcement area
- Responding to AI act application challenges
- Use of the project results to increase the security of the entire European Union
- Close cooperation between LEAs and universities

Name: prof. JUDr. Mojmír Mamojka, PhD. E-mail: mojmir.mamojka@gmail.com

Project participants

Looking for partners with the following expertise/technology/ application field:

- Looking for a strong consortium leader willing to cooperate with:
  - universities focused on ,,Security sciences“ and educating future police officers
  - local LEAs

Part of the Offer of the Police Academy in Bratislava, Slovakia:

- close cooperation not only with the Police Academy, but also with most of the Slovak LEAs (i. a. all parts of Police Presidium) and/or with the Ministry of Interior

Name: prof. JUDr. Mojmír Mamojka, PhD. E-mail: mojmir.mamojka@gmail.com

PAL Robotics

- *Gizem Bozdemir, Senior Project Manager*
- *euprojects@pal-robotics.com*
- *PAL Robotics*

Destination of Interest

- CL3 - CS
  - HORIZON-CL3-2025-02-CS-01
  - HORIZON-CL3-2025-02-CS-02
  - HORIZON-CL3-2025-02-CS-03
  - HORIZON-CL3-2025-02-CS-04
  - HORIZON-CL3-2025-02-CS-05

Needs and interests

HORIZON-CL3-2025-02-CS-01 Generative AI for Cybersecurity applications (RIA)

Secure our AI-driven robots from cyber threats by using generative AI for advanced threat detection and automated defense

HORIZON-CL3-2025-02-CS-02 New advanced tools and processes for Operational Cybersecurity (RIA)

We seeks to strengthen cybersecurity for our robots by integrating real-time monitoring, anomaly detection, and adaptive security for deployment in sensitive environments like healthcare and logistics

HORIZON-CL3-2025-02-CS-03 Privacy Enhancing Technologies (IA)

Implement secure data-handling and privacy-preserving AI for our social and assistive robots to ensure privacy compliance in human-robot interactions

HORIZON-CL3-2025-02-CS-05 Security of implementations of Post-Quantum Cryptography algorithms (IA)

Integrate post-quantum cryptography for secure robot communication and control

Gizem Bozdemir I euprojects@pal-robotics.com

PAL Robotics´ Contribution

Expertise

Navigation	Software	Control	HRI	Electronics	Mechanics	Community	Sales
SLAM Navigation Localization	DevOps Continuous integration	Real Time Manipulation Walking	Social AI Human Perception Interaction Design	Firmware Sensor boards Integration	Bio-inspired and actuation designs Integration	Collaboration Open Source R+D	Flexibility Adaptation Customised solutions

Robotics Platform

Design and manufacture highly integrated robotics solutions

Experiences

Development and Integration

Testing and Validation

Involvement in Similar Projects

CYBER FACTORY NO.1 CF#1

SeCoIIA

PIQASO

Gizem Bozdemir I euprojects@pal-robotics.com

PAL Robotics´ role in the Consortium

PAL Robotics is well-suited to be a **technology provider** in the consortium, **offering robotics platforms for development, testing, and real-world validation** of cybersecurity, AI and cryptographic innovations.

We can act **as an end-user in pilot projects**, ensuring solutions are applicable and scalable for real-world robotic deployments.

Gizem Bozdemir I euprojects@pal-robotics.com

CS-01-02

HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity

Presenters

CS-01-02:

Jordi Herrera-Joancomartí *jordi.herrera@uab.cat*
Raúl Orduna-Urrutia *rorduna@vicomtech.org*
Rita Nogueira *rita.nogueira@treetk.com*
Mario Pichler *mario.pichler@scch.at*

BLOCKSHIELD: AI-Driven Defense Against Ransomware and Hybrid Cyber Threats

- Jordi Herrera-Joancomartí
- jordi.herrera@uab.cat
- *Universitat Autònoma de Barcelona*

- Role: *WP Leader (Work Package: Blockchain Analysis & Cyber Threat Intelligence)*
- Topic to be addressed: *CL3-2025-02-CS-02*

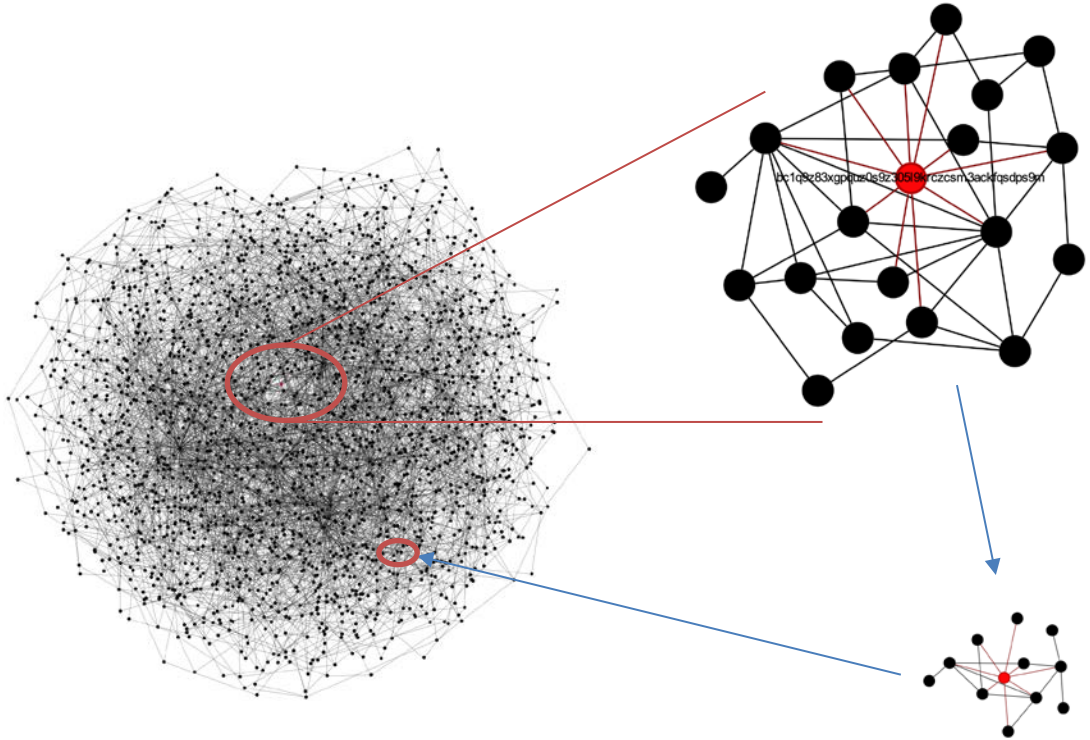
BLOCKSHIELD: AI-Driven Defense Against Ransomware and Hybrid Cyber Threats

- *Objective of our Work Package:*
  - *Develop **AI-based techniques to detect and trace suspicious blockchain transactions**, focusing on **ransomware payments and command-and-control (C&C) mechanisms**.*

- *Key Contributions as WP Leader:*
  - ***Tracing cryptopayments with advanced GNN techniques** to uncover illicit blockchain transactions.*
  - *Developing a forensic tool to analyze ransomware **TTPs (Tactics, Techniques, and Procedures)** on blockchain ecosystems.*
  - ***Building an AI-powered framework** for **threat intelligence and early detection** of hybrid cyber threats.*

Jordi Herrera-Joancomartí jordi.herrera@uab.cat

BLOCKSHIELD: AI-Driven Defense Against Ransomware and Hybrid Cyber Threats



Jordi Herrera-Joancomartí jordi.herrera@uab.cat

Project participants

- Existing consortium:
  - Proposed coordinator: *Not yet*
  - Partners / Other:
    - UAB, ES (Blockchain and GNN development)
- Looking for partners with expertise in:
  - ***Coordination***
  - ***Forensics & Compliance****: Blockchain AML and forensic analysis.*
  - ***Law Enforcement / Gov. Agency****: Validation, real-world testing.*
  - ***Testing & Experimentation Provider****: Cyber ranges, ransomware sandbox.*
  - ***Financial Sector****: Banking & financial fraud detection.*
  - ***Ethics & Legal Experts****: Regulatory compliance & privacy.*

Jordi Herrera-Joancomartí jordi.herrera@uab.cat

Supply Chain Wireless SOC

- *Raúl Orduna-Urrutia*
- *rorduna@vicomtech.org*
- *VICOMTECH*
- *WP leader*

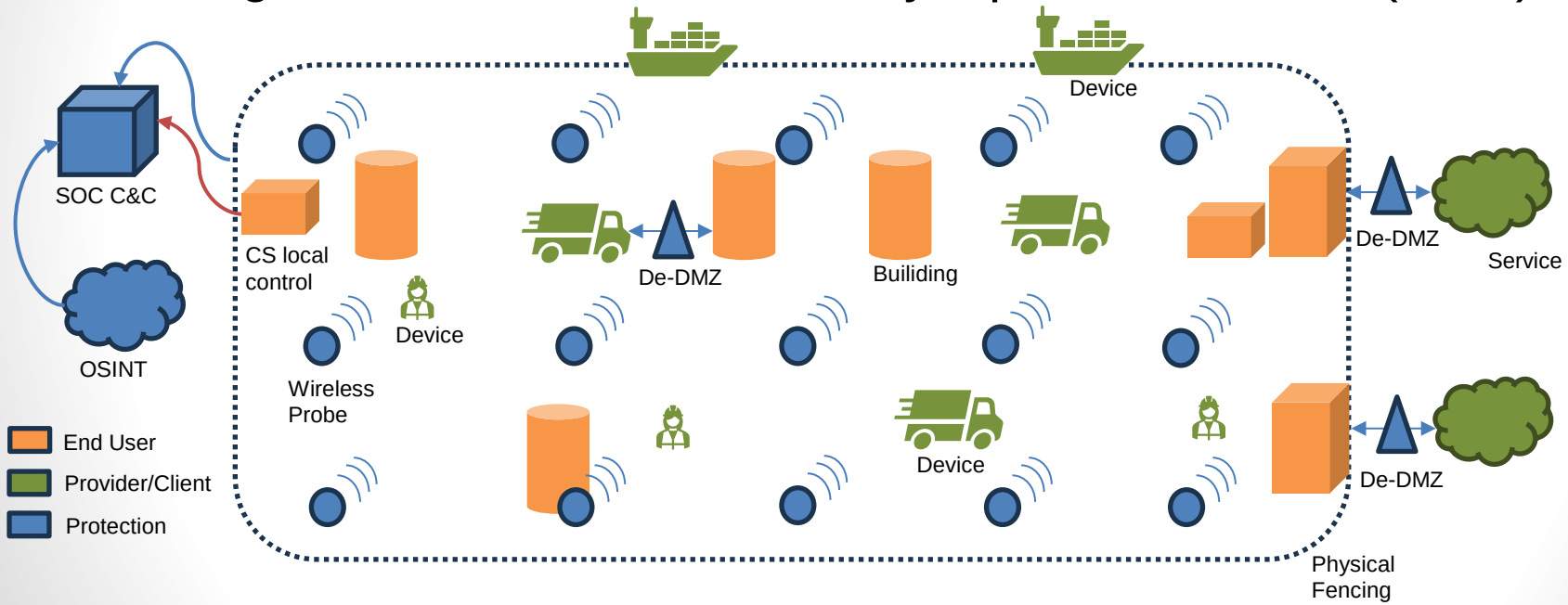
- Topic to be addressed: *CL3-2025-02-CS-02*

"New advanced tools and processes for Operational Cybersecurity"

Proposal related to RED directive, increasing situational awareness in wide area locations

Proposal idea/content

- Design and deploy a wireless grid of sensors to feed and integrate in a dedicated Security Operation Centre (SOC)



Project participants

- Existing consortium:
  - Proposed coordinator: Not yet
  - Partners / Other participants:
    - Cyber security analysis of Wireless Communication
    - Extend DMZ to exposition surface with supply chain agents
    - OSINT automatic extraction related to suppliers
    - Spanish End User, transport sector
- Looking for partners with the following expertise/ technology/ application field:
  - SOC managers (Lead)
  - Radio Electric manufacturer and embedded systems developer
  - Evaluator/Certifier organization for cybersecurity devices
  - End user, wide area controllers

PREACT – Predictive Digital Twins for Proactive Cybersecurity Response

- *Santiago Macho González, Rita Nogueira*
- *santiago.macho@treetk.com; rita.nogueira@treetk.com*
- *Tree Technology*
  - Spanish SME
  - Field of expertise: Big Data, AI, Cybersecurity
  - >30 EU projects. 10 (EU) ongoing +6 national PPI on cybersecurity
  - 10 projects on H2020-SEC. 3 ongoing: TRUSTaWARE, TeamAware and Nightingale.
  - 3 proposals under HE-CL3 recently approved

- Role: *Proposal coordinator, WP leader, S/T provider*

- Topic to be addressed: *CL3-2025-CS-02*

Proposal idea/content

- ***Motivation****: SOC teams lack safe, realistic environments to anticipate and test responses, leaving them in a reactive cybersecurity posture.*
- ***Objective****:* Develop advanced digital twins of critical infrastructure using real-time SCADA/OT data integrated with AI-driven predictive simulations, enabling proactive cybersecurity response and enhanced resilience.
- ***Methodology****:*
  - **Real-time Data Integration:** Continuously integrate SCADA/OT system data into virtual digital twins of critical infrastructure.
  - **Predictive Simulations:** Apply AI and Machine Learning to anticipate cyber-attacks, assess potential impacts, and simulate defensive scenarios proactively.
  - **Automated Decision Support:** Generate prioritized recommendations and response strategies without disrupting live operations.

Physical **Digital Twin**

Rita Nogueira (*rita.nogueira@treetk.com*) / Santiago Macho (*santiago.macho@treetk.com*)

Project participants

- Existing consortium:
  - TREE as expertise in cybersecurity / AI (WP leader / coordinator)

- Looking for partners with the following expertise/ technology/ application field:
  - Looking for a coordinator
  - Digital twin platform developer
  - SCADA/OT System Providers
  - End users (SOCs, CSIRTs, and critical infrastructure operators energy, transport, healthcare,..)

Rita Nogueira (*rita.nogueira@treetk.com*) / Santiago Macho (*santiago.macho@treetk.com*)

- *Mario Pichler*
- *mario.pichler@scch.at*
- *Software Competence Center Hagenberg GmbH*
- Role: *WP leader*

- Topic to be addressed: ***HORIZON-CL3-2025-02-CS-ECCC-02*** *New advanced tools and processes for Operational Cybersecurity*

Proposal idea/content

An AI model designed by our project partners to enhance cybersecurity will necessarily integrate critical company-specific knowledge. This information can become a **primary target** for adversaries**.**

- **Protecting Sensitive Knowledge:** Addressing risks from company-specific security data contained in AI models
- **Model Security Focus:** Preventing model stealing & inference attacks
- **Adversarial Defense:** Detecting and automatically responding to attacks
- **Dynamic Adaptation:** Adjusting model behavior upon threat detection

Proposal idea/content

Our strengths:

- Strong connections with key industry partners
- Years of experience in protecting AI models, including several publications
- Deep expertise in data science and IT security, with a focus on IP protection

Other topics of interest:

- AI-supported risk assessment
- AI jailbreaking
- Exploit code generation for automated security testing

Project participants

- Looking to join an existing consortium with the following expertise/ technology/ application field:
  - Ability and knowledge to develop and train new generative AI models
  - Capability to provide the necessary (training) data to support the research
  - Expertise in legal aspects concerning both EU and national regulations

CS-01-03

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing TechnologiesCybersecurity Presenters

CS-01-03:

Petr Dzurenda *dzurenda@vut.cz*
Cristina Pérez-Solà *cristina.perez@uab.cat*
Aitor Corchero *aitor.corchero@eurecat.org*

- *Dr. Petr Dzurenda*
- *dzurenda@vut.cz*
- *Brno University of Technology, Czech Republic*

- Role: *WP leader*

- Topic to be addressed: CL3-CS-02-03: **Privacy Enhancing Technologies**

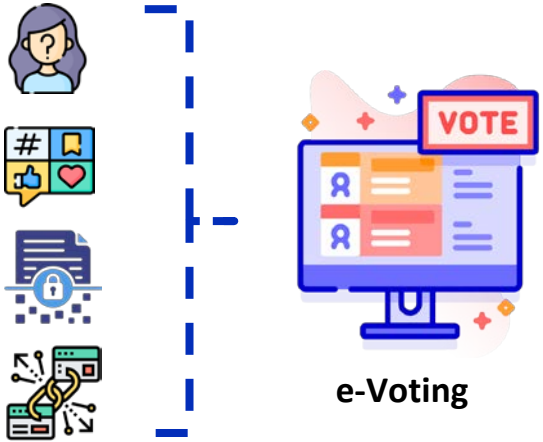
Proposal idea/content

PETs for European Digital Identity

The privacy-preserving crypto-agile module for EUDI Wallet and Democracy

EU Digital Identity Wallet

- **Anonymous Credentials**
  selective disclosure and unlinkability
- **Zero-Knowledge Proofs (zkSNARKs)**
  prove a statement is true
- **Homomorphic Encryption**
  computations on encrypted data
- **Blockchain**
  transparency, availability, and trust



e-Voting

Cryptographic algorithms suitable for constrained devices such as smart cards:

Camenisch J, Drijvers M, Dzurenda P, Hajny J. Fast keyed-verification anonymous credentials on standard smart cards. InICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34 2019 (pp. 286-298). Springer International Publishing.

Project participants

- Existing consortium:
  - Proposed coordinator: ***TBD***
  - Partners / Other participants: ***TBD***

- **Cryptographic Protocol Design** and **Applied Cryptography** :
  - PETs (anonymous credentials, zero-knowledge proofs, **authentication**),
  - **Data Privacy** (differential privacy, k-anonymity)
  - Apps for **smart cards**, **smartphones**, wearables, MCU.
- **We are part of** :

SPARTA CHESS REWIRE Cybersecurity Skills Alliance Digital4Security Shaping Europe's cyber future EULiST

Contact us!

Dr. Petr Dzurenda

Email: dzurenda@vut.cz

Brno University of Technology

Academic institution

Czech Republic

Websites: https://axe.vut.cz/

Privacy-Enhancing Decentralized Technologies for Secure Data Processing

- Cristina Pérez-Solà
- cristina.perez@uab.cat
- *Universitat Autònoma de Barcelona*

- Role: *WP Leader (Work Package: Blockchain-Based Privacy Enhancing Technologies)*
- Topic to be addressed: *CL3-2025-02-CS-03*

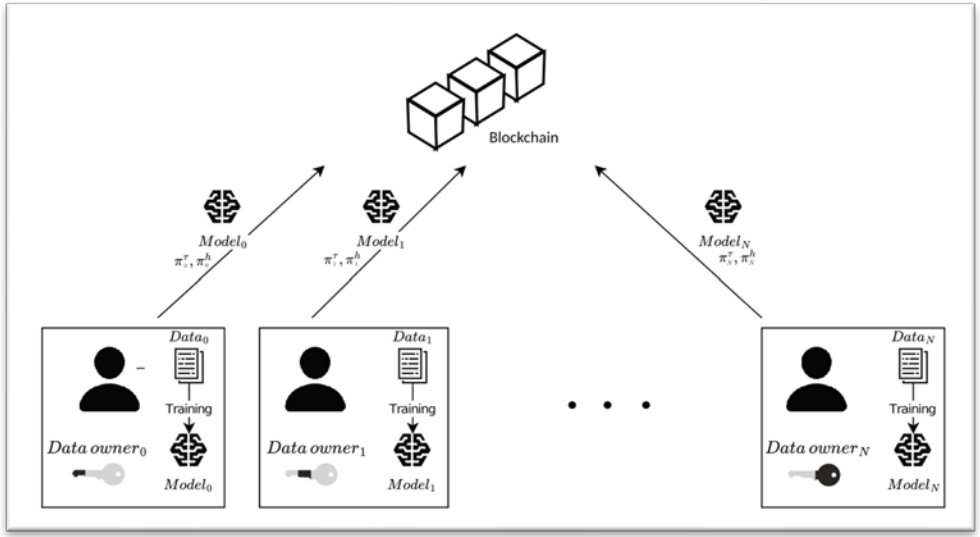
Privacy-Enhancing Decentralized Technologies for Secure Data Processing

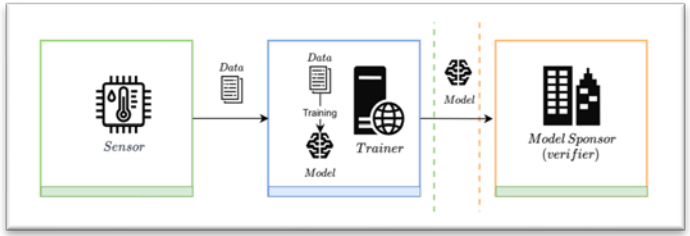
- *Objective of Work Package:*
  - *Develop **blockchain-based and decentralized privacy-enhancing technologies** to ensure **secure and privacy-preserving data processing** in decentralized environments.*
  - *Combine **blockchain with federated learning**, addressing **data security and privacy concerns** in machine learning applications.*
  - *Facilitate the **transition to quantum resistant cryptographic algorithms**, ensuring long-term security in decentralized applications.*

- *WP Contributions:*
  - *Designing **secure and private decentralized federated learning** frameworks on blockchain.*
  - *Building **crypto-agile key derivation schemes** for **secure blockchain wallet** management, ensuring transition to **post-quantum cryptographic** algorithms.*
  - *Application of derivation schemes in **identity wallets aligned to EDS** identity management architecture*
  - *Integrating **zero-knowledge** primitives to preserve privacy while enabling **verifiable execution**.*
  - *Integration of secret sharing schemes for **efficient and supervised computation***

Cristina Pérez-Solà cristina.perez@uab.cat

Privacy-Enhancing Decentralized Technologies for Secure Data Processing





Cristina Pérez-Solà cristina.perez@uab.cat

Project participants

- Existing consortium:
  - Proposed coordinator: Not yet
  - Partners / Other participants:
    - Spanish UN, experts in decentralized processing and Zero-knowledge proofs
    - Spanish RTO, efficient secure protocols (SMC) and EDS identity management
- Looking for partners with the following expertise/ technology/ application field:
  - Secure Cloud Service Provider (Lead)
  - European Data Space Infrastructure operator
  - TSP/HSM manufacturer or integrator
  - End users: Health Data provider through EDS
  - Developer of Standards
  - Ethics and privacy experts

Cristina Pérez-Solà cristina.perez@uab.cat

PRIMES- Mesh for Secure, Scalable, and Sovereign Data Ecosystems

HORIZON-CL3-2025-02-CS-03: Privacy Enhancing Technologies

Aitor Corchero – Innovation Manager at IT&OT Security
[Ideas- WP Leader/Partner]

"innovating with businesses"

Our Idea: PRIMES

- **Creating Privacy as a backbone-** Combination of identity, AI and Blockchain technology.
- **From Compliance to Confidence-** Using Distributed Credentials, Federated AI and Privacy-Preserving Data by Design.
- **Zero Data Exposure-** Combining Differential Privacy + Federated Learning + Verifiable Credentials for real-world adoption.
- **Scalable Trust. Embedded Privacy-** Built on Federated Learning and Differential Privacy, governed by Decentralized Identity.

Join our Journey

- **From lab to field**: our PET stack combines Differential Privacy, Federated Learning, and Verifiable Credentials tested in EU projects.
- **We make PETs usable, compliant, and scalable** - solving the very gap this call is meant to address
- **Post-Quantum resistant PETS**- research on post-quantum PETs applied to dataspaces (PLIADES)

SMI2G
Security Mission Information & Innovation Group

Let's lead the next wave of EU cybersecurity innovation together

Contact: Aitor Corchero
Eurecat | aitor.corchero@eurecat.org

CS-01-05

HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

Presenters

CS-01-05:

Aitor Corchero *aitor.corchero@eurecat.org*

Post-Quantum Resilience for Low-Power Systems (LITECRYPT)

HORIZON-CL3-2025-02-CS-05: Security of implementations of Post-Quantum Cryptography algorithms

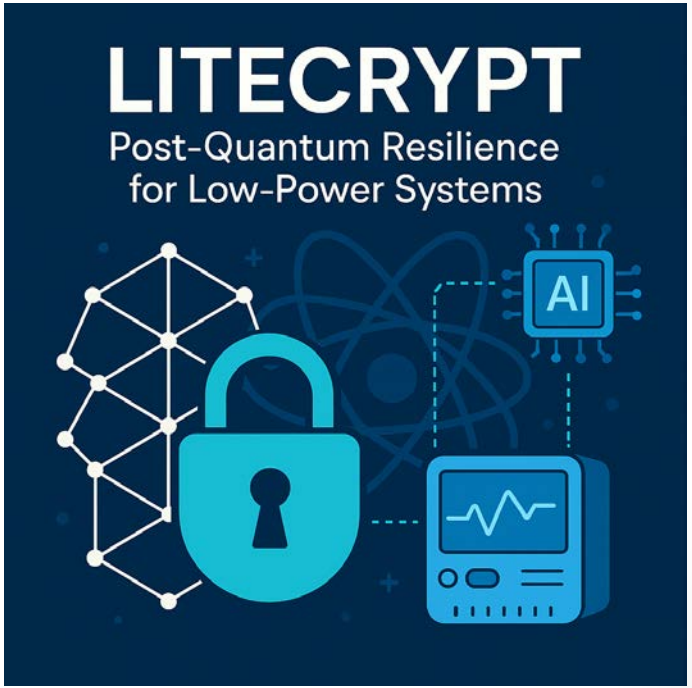
Aitor Corchero – Innovation Manager at IT&OT Security
[Ideas- WP Leader/Partner]

"innovating with businesses"

Our Contribution: LITECRYPT

The Challenge

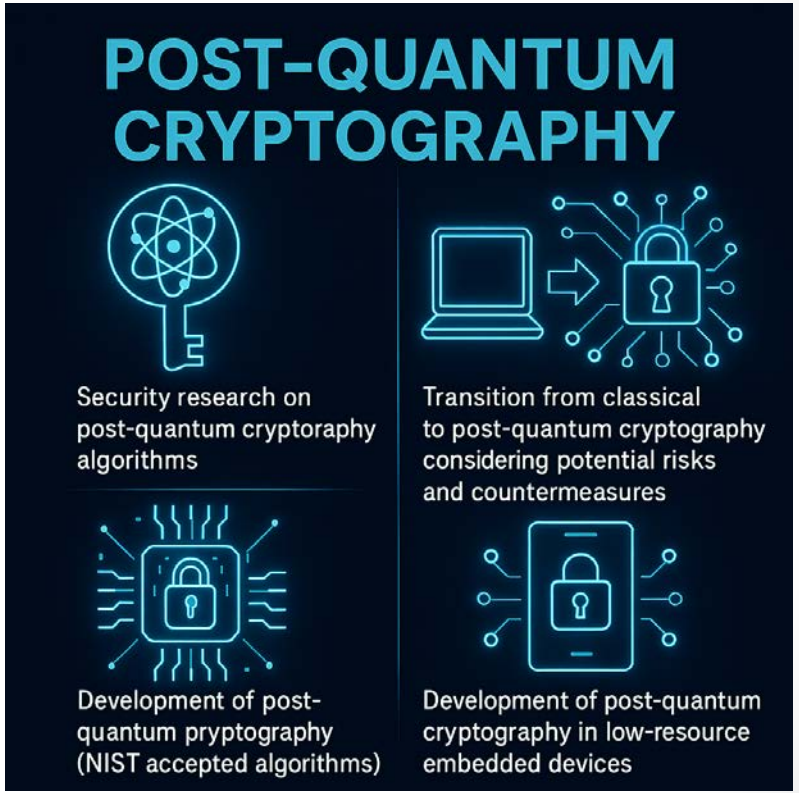
- **Unprotected targets with low-power & low-cost devices –** Main efforts focused on high-resource systems**.**
- **Emerging threat-** IoT/IIoT systems backbone part of the critical infrastructures and PQC remain untested.
- **Urgently need post-quantum cryptographic strategies that work for resource-constrained environments**



Our Contribution: LITECRYPT

Our Proposed Contribution

“From NIST-compliant cryptography to low-power systems, we make post-quantum security practical, scalable, and future-proof.”



Join our Journey

- AI-enhanced quantum threats to real-world protection of critical infrastructures and embedded systems.
- Let’s prepare to the future, let’s make quantum resilience real.

Let’s lead the next wave of EU cybersecurity innovation together

Contact: Aitor Corchero
Eurecat | aitor.corchero@eurecat.org

CS-01-06

HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Presenters

CS-01-06:

Sara Ricci *ricci@vut.cz*

- *Dr. Sara Ricci*
- *ricci@vut.cz*
- *Brno University of Technology, Czech Republic*
- Role: *WP leader*

- Topic to be addressed: CL3-CS-02-06: **Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols**

Proposal idea/content

Quantum Safe Authentication for Europe

Towards quantum safe authentication using constrained devices

Constrained Devices

- **Password-Authenticated Key Exchange (PAKE)**
  - ✓ Protocols such as: SRP, SPAKE2, and WPA3-SAE
- **Threshold signature**
  - ✓ Protocols such as: FIDO2 (WebAuthn), OAuth 2.0
- **KEMs and Digital signatures**
  - ✓ CRYSTALS-Dilithium & Kyber for microcontrollers and smart cards (2FA)
- **End to End Encryption Protocols**
  - ✓ Protocols such as: Signal and Noise

User Authentication

*Cryptographic protocols suitable for **constrained devices** such as smart cards and secure elements, **combining current and post-quantum** algorithms for backward compatibility*

Project participants

- Existing consortium:
  - Proposed coordinator: ***TBD***
  - Partners / Other participants: ***TBD***
  - s
- **Cryptographic Protocol Design** and **Applied Cryptography** :
  - Authentication and identification protocols
  - PQC (CRYSTALS-**Dilithium** & **Kyber**, DS2),
  - PQC transition mechanisms (KEM combiners),
  - Apps for **smart cards**, smartphones, wearables, MCU, **FPGA**.
- **We are part of** :

SPARTA CHESS REWIRE Cybersecurity Skills Alliance Digital4Security Shaping Europe's cyber future EULiST

Contact us!

Dr. Sara Ricci

Email: ricci@vut.cz

Brno University of Technology

Academic institution

Czech Republic

Websites: https://axe.vut.cz/