IDUNN

INDUSTRIAL CYBERSECURITY

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

PROJECT OVERVIEW

Project No:	101021911
Project Full Name:	A Cognitive Detection System for Cybersecure Operational Technologies
Duration	36 months
Start Date	September 2021
Partnership	10 partners
Program	Horizon 2020
Budget	EUR 4 909 745

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN is focusing on adding the trust ingredient to any business by making its ICT systems **resilience to cyber-attacks**. It will create a **security shield** in the form of tools, methodologies, microservices and initial standards compatible with any ICT supply chain. The project will demonstrate a secure Continuity Plan for ICT based organisations by creating and validating a unique **Cognitive Detection System for Cybersecure Operational Technologies**.

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

OBJECTIVES

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

Add a TRUST ingredient to any business by making its ICT systems resilience to cyber-attacks

TRUSTWORTHY
Increase trust in both IT and OT

FASTER
Increase response and lower recovery time

EFFORTLESS
Decrease person effort to ensure cybersecurity

PRODUCTIVE
Have a crucial impact in productivity

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

PROJECT PARTNERS

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

Finland

Bittium

UNIVERSITY OF OULU

Germany

OFFIS INSTITUTE FOR INFORMATION TECHNOLOGY

CoSynth

DIN

France

MONDRAGON ASSEMBLY

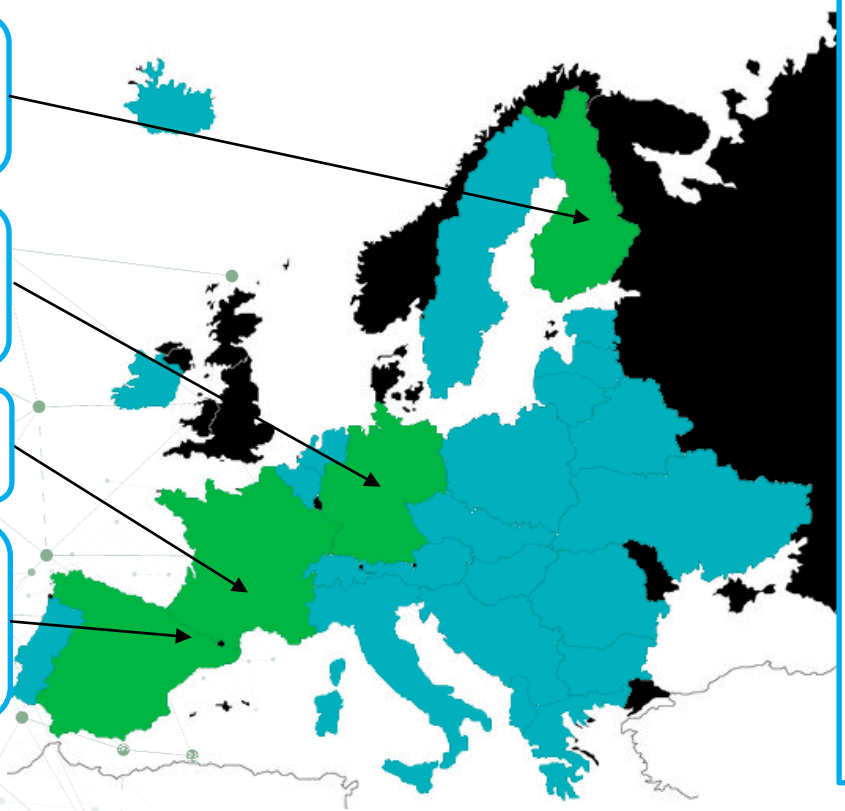
Spain

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

S21SEC

FAGOR ARRASATE

GAIA CLUSTER ICTA



- IKERLAN (LEADER)
- GRUPO S 21SEC GESTION
- FAGOR ARRASATE
- GAIA
- OULUN YLIOPISTO
- BITTIUM WIRELESS
- MONDRAGON ASSEMBLY
- OFFIS
- DIN DEUTSCHES INSTITUT
- FUERNORMUNG
- COSYNTH GMBH

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

RESULTS

- A **methodology** based on an immutable blueprint that guarantees the integrity and traceability of a complex ICT system
- A holistic **threat model** at the light of the MITRE TTP of the ICT supply chain in complex ICT/OT environments
- A validated technological **security framework** in the form of tools and microservices to enable automatic and dynamic cybersecurity operations:
- A complete **integration plan** based on three main project scenarios as an example of their applicability on other general ICT supply systems
- **Co-creation activities** with potential stakeholders (starting with the IDUNN three scenarios) to reduce and standardise the human intervention and tools proposed as a means to ensure resilience on ICT complex systems through certification

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

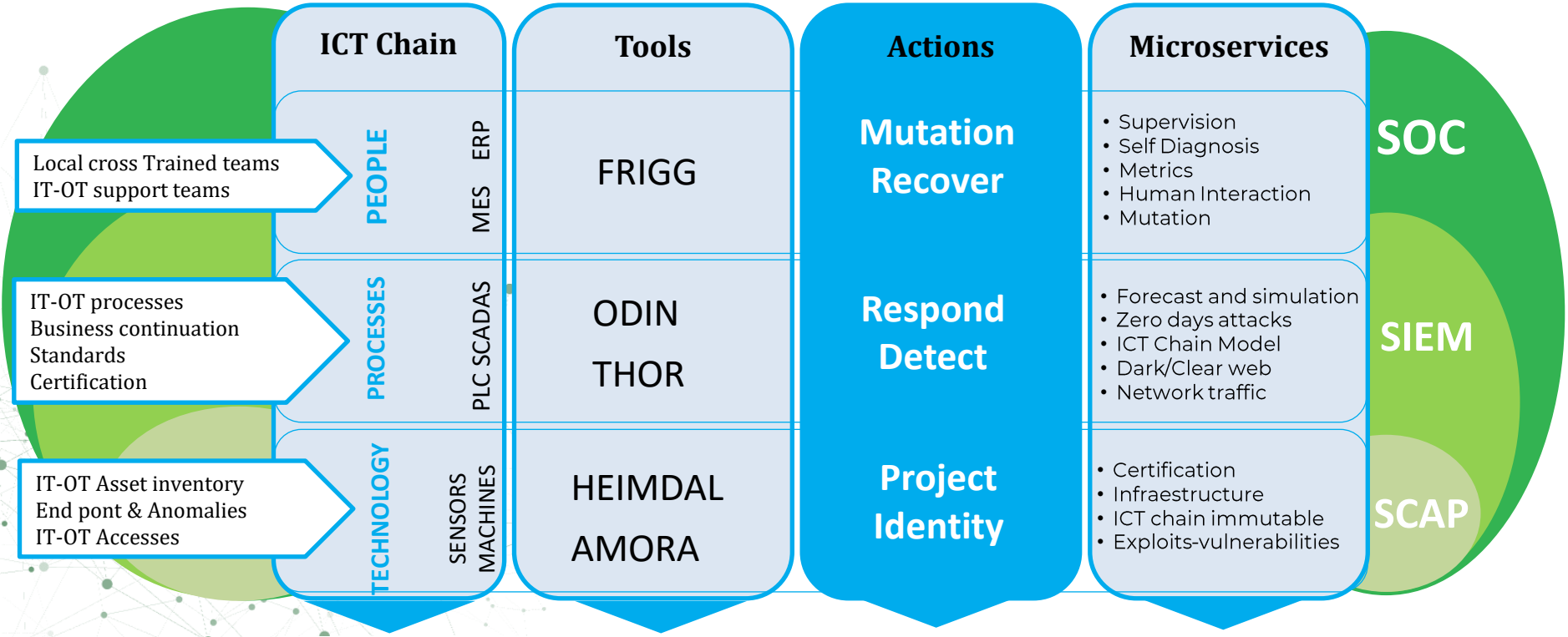
IDUNN' PILLARS

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

IDUNN'S STRUCTURE

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES



Energy sector
Manufacturing sector
Transport sector

Advanced cybersecurity products
Increase TRUS in ICT components
Less effort to assure a compliance

Increase citizen privacy
Improve EU market opportunities
Harmonized certification schemes

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

IDUNN'S FRAMEWORK

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

1. AMORA

Fingerprinting of the OT components by profiling interfaces and behaviours, testing for interfaces compliance to profiles, certification documentation, testing data.

3. THOR

Centrally detection of "unknown" or "zero-day" threats through fair IA and data analytics.

5. FRIGG

Run a self-diagnostic operation according to certain metrics and goals

2. HEIMDAL

Automated discovery of known threats, detection at the endpoint.

4. ODIN

Run resilience actions (Response, Recovery, Mitigation) against the threats detected through THOR

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

USE CASES

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

APPLICATION FOR AVIATION LIGHTNING OF WIND ENERGY PLANTS

MANUFACTURING OF GAS VALVES FOR HOUSEHOLD APPLICATION IN ENERGY SECTOR

AUTOMOTIVE MECHANICAL AND HYDRAULIC PRESSES

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911

IDUNN
INDUSTRIAL CYBERSECURITY

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

THANK YOU!

www.idunnproject.eu

@Idunnproject

IDUNN project

idunn-project

This project has received funding form the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021911