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

OBJECTIVES

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

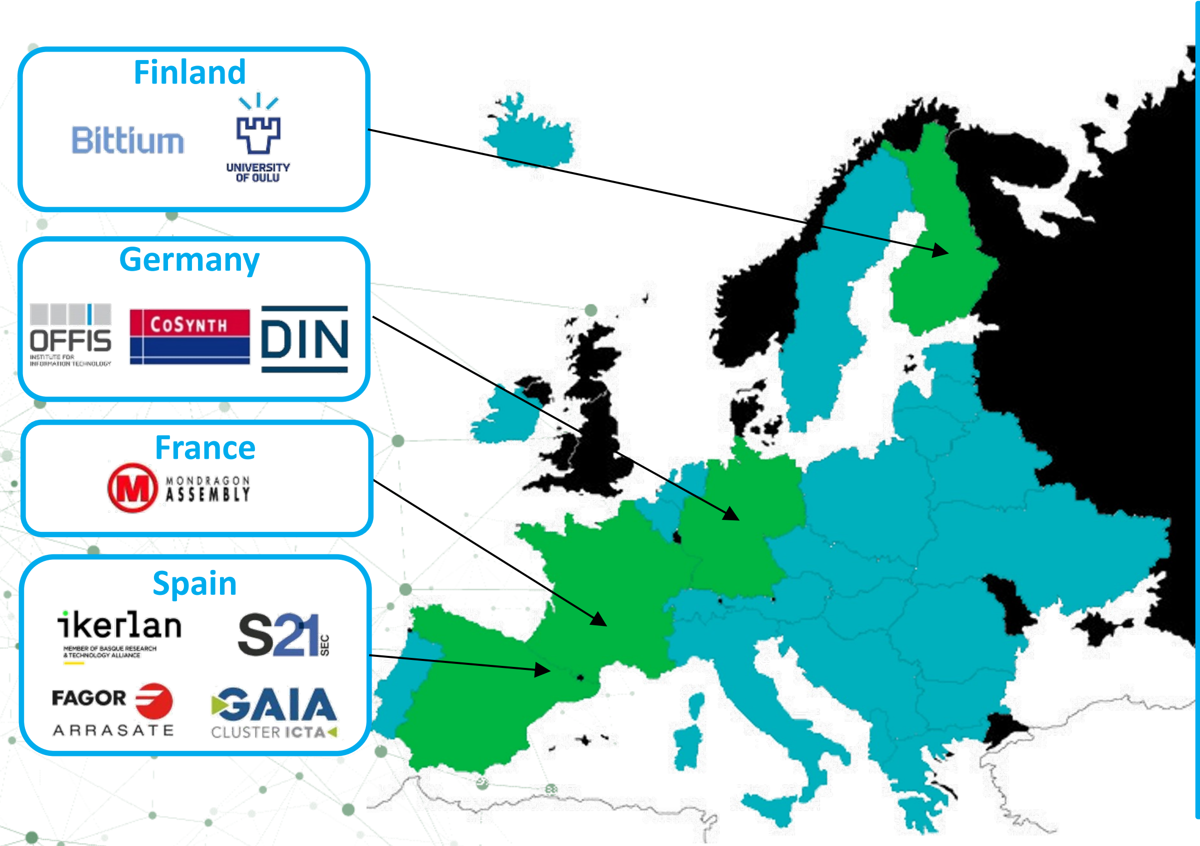
PRODUCTIVE
Have a crucial impact in productivity

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



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

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

IDUNN’S PILLARS

1. IDENTIFICATION (AUTOMATED AUDIT)

2. PROTECTION, POLICY ENFORCERS, ACTIVITY MONITORS

3. AI DYNAMIC ANOMALY DETECTION

4. AI-BASED RISK MODELS

5. RESPONSE, RECOVERY AND INFORM

6. SELF-DIAGNOSIS HUMAN INTERVENTION

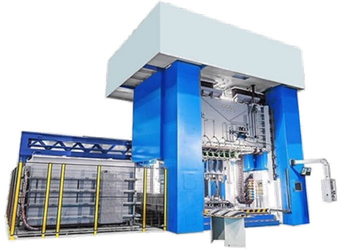
7. CONTRIBUTION TO STANDARDS

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

USE CASES

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

INDUSTRIAL CYBERSECURITY

IDUNN’S FRAMEWORK

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

AMORA

1.

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

HEIMDAL

2.

Automated discovery of known threats, detection at the endpoint.

THOR

3.

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

ODIN

4.

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

FRIGG

5.

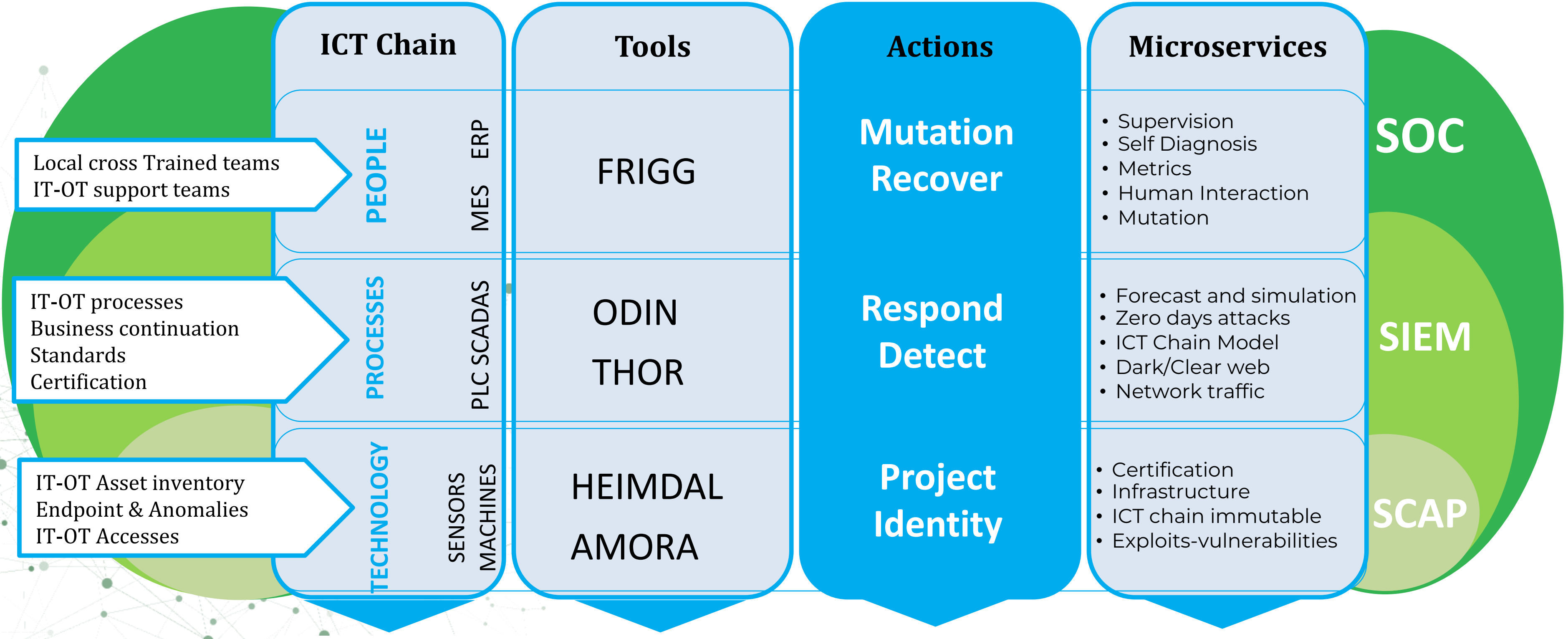
Run a self-diagnostic operation according to certain metrics and goals

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



	ICT Chain	Tools	Actions	Microservices	
Local cross Trained teams IT-OT support teams	PEOPLE MES ERP	FRIGG	Mutation Recover	• Supervision • Self Diagnosis • Metrics • Human Interaction • Mutation	SOC
IT-OT processes Business continuation Standards Certification	PROCESSES PLC SCADAS	ODIN THOR	Respond Detect	• Forecast and simulation • Zero days attacks • ICT Chain Model • Dark/Clear web • Network traffic	SIEM
IT-OT Asset inventory Endpoint & Anomalies IT-OT Accesses	TECHNOLOGY SENSORS MACHINES	HEIMDAL AMORA	Project Identity	• Certification • Infrastructure • ICT chain immutable • Exploits-vulnerabilities	SCAP

Energy sector
Manufacturing sector
Transport sector

Advanced cybersecurity products
Increase TRUST 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

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

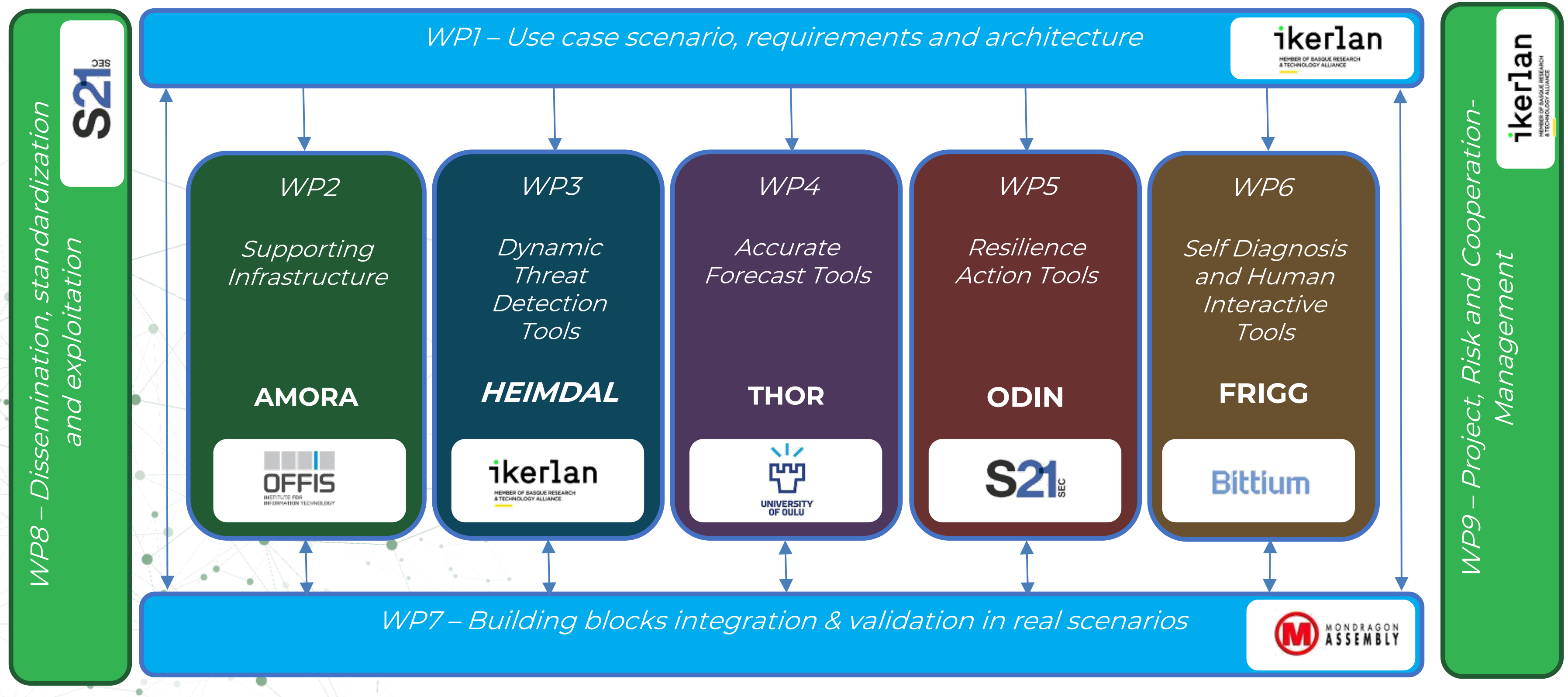
- **Co-creation activities** with potential stakeholders (starting with the IDUNN three scenarios) to reduce and standardise the human intervention and tools proposed as a means to ensure resilience on ICT complex systems through certification

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

IDUNN
INDUSTRIAL CYBERSECURITY

A COGNITIVE DETECTION SYSTEM FOR CYBERSECURE OPERATIONAL TECHNOLOGIES

PROJECT STRUCTURE



WP1 – Use case scenario, requirements and architecture

ikerlan

WP2

Supporting Infrastructure

AMORA

OFFIS

WP3

Dynamic Threat Detection Tools

HEIMDAL

ikerlan

WP4

Accurate Forecast Tools

THOR

UNIVERSITY OF OULU

WP5

Resilience Action Tools

ODIN

S21 SEC

WP6

Self Diagnosis and Human Interactive Tools

FRIGG

Bittium

WP7 – Building blocks integration & validation in real scenarios

MONDRAGON ASSEMBLY

WP8 – Dissemination, standardization and exploitation

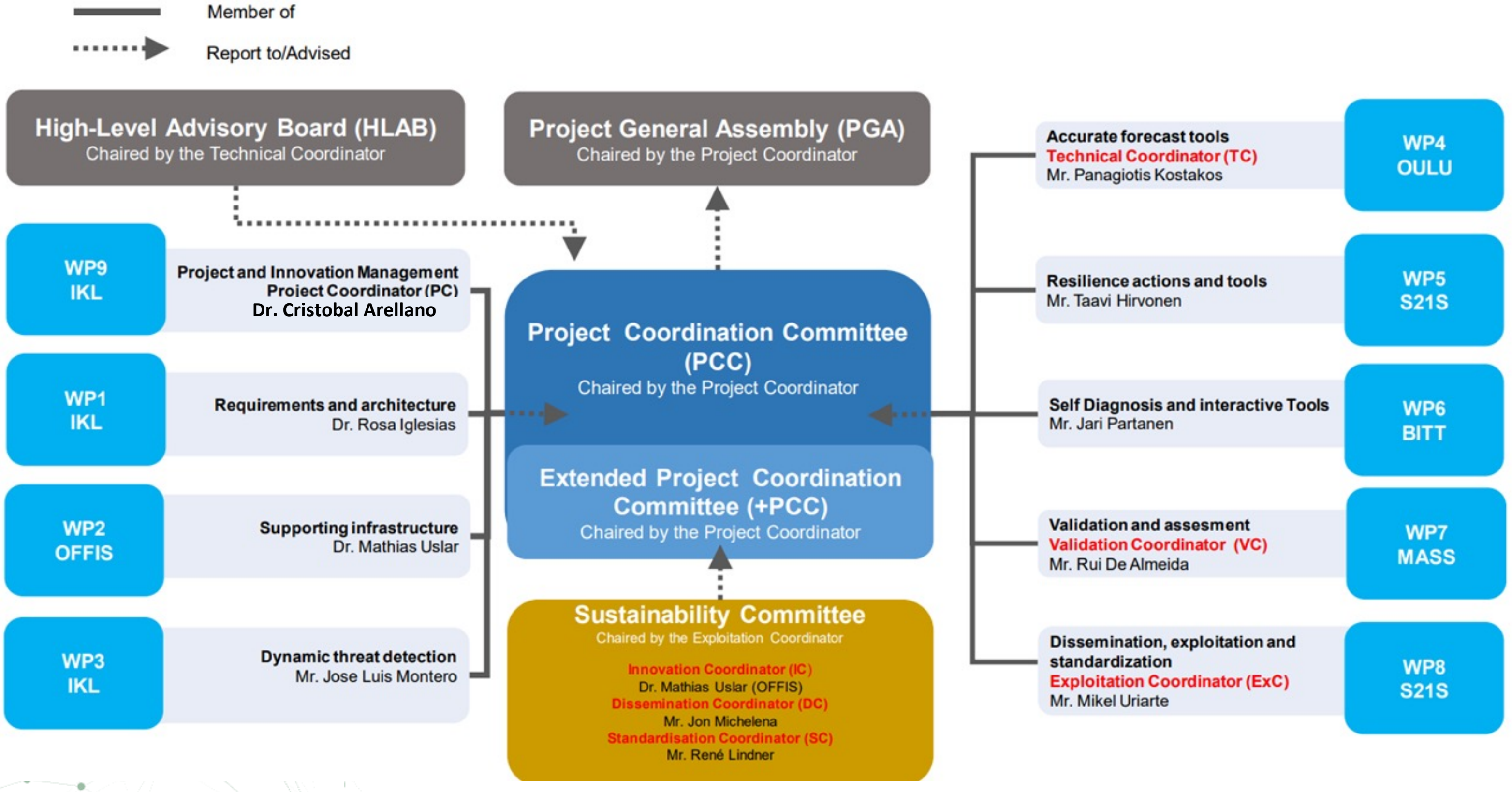
S21 SEC

WP9 – Project, Risk and Cooperation-Management

ikerlan

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

MANAGEMENT STRUCTURE & ROLES



Member of

Report to/Advised

High-Level Advisory Board (HLAB)
Chaired by the Technical Coordinator

Project General Assembly (PGA)
Chaired by the Project Coordinator

Project Coordination Committee (PCC)
Chaired by the Project Coordinator

Extended Project Coordination Committee (+PCC)
Chaired by the Project Coordinator

Sustainability Committee
Chaired by the Exploitation Coordinator
Innovation Coordinator (IC)
Dr. Mathias Uslar (OFFIS)
Dissemination Coordinator (DC)
Mr. Jon Michelena
Standardisation Coordinator (SC)
Mr. René Lindner

WP9 IKL
Project and Innovation Management
Project Coordinator (PC)
Dr. Cristobal Arellano

WP1 IKL
Requirements and architecture
Dr. Rosa Iglesias

WP2 OFFIS
Supporting infrastructure
Dr. Mathias Uslar

WP3 IKL
Dynamic threat detection
Mr. Jose Luis Montero

WP4 OULU
Accurate forecast tools
Technical Coordinator (TC)
Mr. Panagiotis Kostakos

WP5 S21S
Resilience actions and tools
Mr. Taavi Hirvonen

WP6 BITT
Self Diagnosis and interactive Tools
Mr. Jari Partanen

WP7 MASS
Validation and assesment
Validation Coordinator (VC)
Mr. Rui De Almeida

WP8 S21S
Dissemination, exploitation and standardization
Exploitation Coordinator (ExC)
Mr. Mikel Uriarte

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