MEDITERRANEAN SECURITY EVENT 2019

DEFENDER

Combining cyber and physical security management for critical energy infrastructure protection: the DEFENDER project

DR. ARTEMIS VOULKIDIS – POWER OPERATIONS LIMITED

DEFENDER IDENTITY CARD

CALL IDENTIFIER: H2020 CIP-2016-2017-1

TITLE: ***DEFENDING THE EUROPEAN ENERGY INFRASTRUCTURES***

STARTING DATE: 1 MAY 2017

ACTION TYPE: *INNOVATION ACTION*

DURATION: *36 MONTHS (CLOSING DATE: 30/4/2020)*

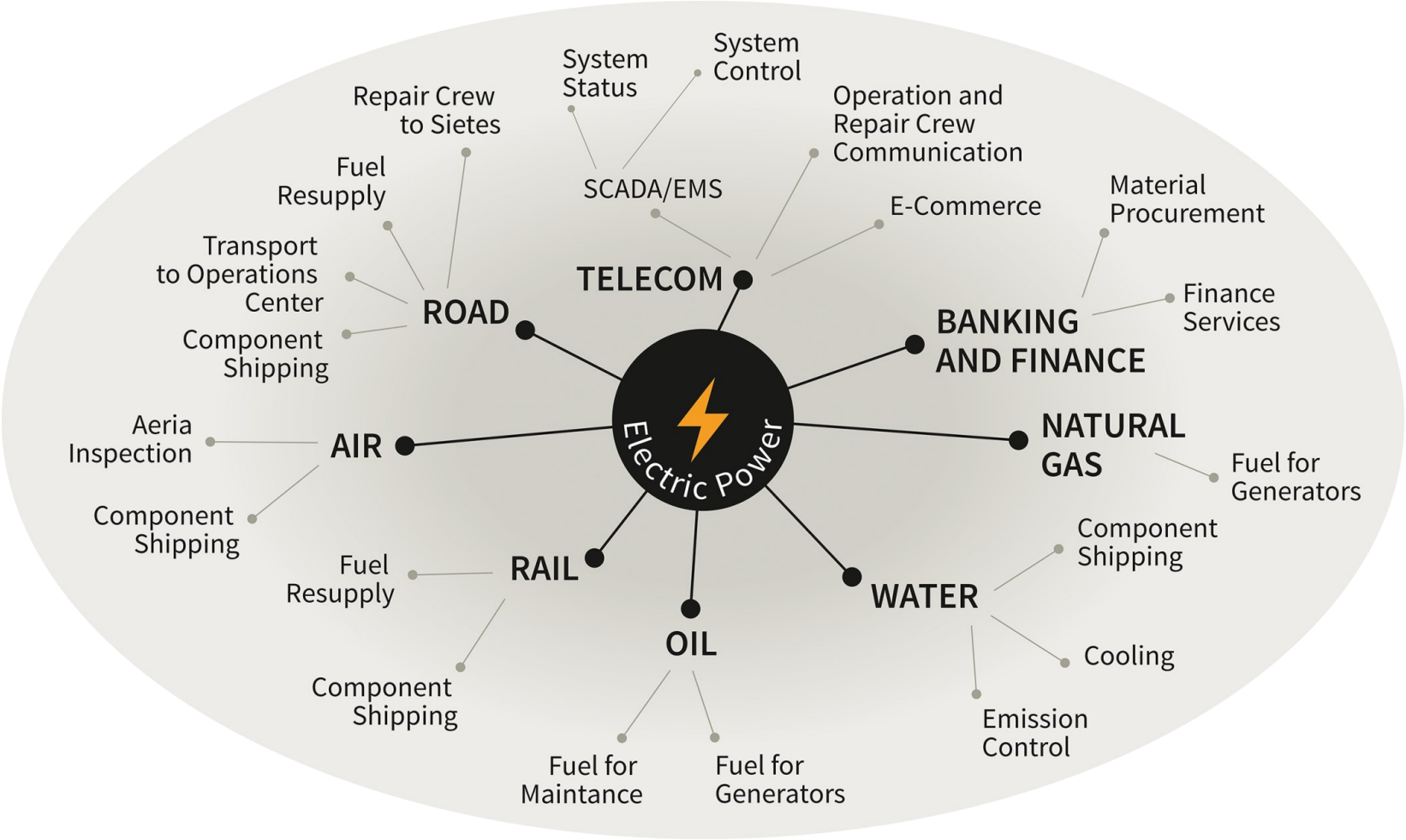
EU CONTRIBUTION: 6.790.837,50 €

PARTNERS: 18 (FROM **9** COUNTRIES)

COUNTRY COVERAGE: *ITALY, GREECE, FRANCE, ROMANIA, GERMANY, SLOVENIA, PORTUGAL, UK, ISRAEL*

WEBSITE: *HTTP://DEFENDER-PROJECT.EU/*

CRITICAL ENERGY INFRASTRUCTURES (CEI)



DEFENDER OBJECTIVES

ANALYSE CEI **THREATS AND RISKS**, CREATE METHODOLOGY FOR PREDICTING **NEW/YET UNKNOWN** RISKS

GAIN CEI SITUATION **AWARENESS**, **PERCEPTION** AND **COMPREHENSION** BY INTERFACING PHYSICAL, CYBER & HUMAN/VIRTUAL SENSORS AND METERING DEVICES AND BY UTILISING A CYBER-PHYSICAL SOCIAL SYSTEM (CPSS) CO-SIMULATOR

DEVELOP METHODOLOGIES AND TOOLS FOR INNOVATIVE, **TRUSTED**, **PRIVATE** AND **TRACEABLE BIDIRECTIONAL INFORMATION FLOWS**

INTEGRATE DYNAMIC THREAT, VULNERABILITY ANALYSIS AND ATTACK DETECTION TO TRIGGER THE **MOST SUITABLE COUNTERMEASURES**

COORDINATE, SYNCHRONIZE AND CROSS-VALIDATE INFORMATION SHARING AND EXCHANGE ON PHYSICAL AND CYBER ATTACKS PATTERNS AND COUNTERMEASURES, VIA A **CEI INCIDENTS INFORMATION SHARING PLATFORM (I2SP)**

COORDINATE THE CRITICAL ENERGY INFRASTRUCTURE SECURITY STAKEHOLDERS GROUP (CEIS-SG)

STRATEGIC-LEVEL APPROACHES

CEI SECURITY "BY-DESIGN"

- SELF-HEALING (E.G. FAULT-LOCATION /RESTORATION)
- DATA PROTECTION (E.G. CRYPTOGRAPHY/BLOCKCHAINS)
- SECURITY ASSESSMENT LIFECYCLE ASSESSMENT
- RISK IMPACT VS THREAT MATRIX

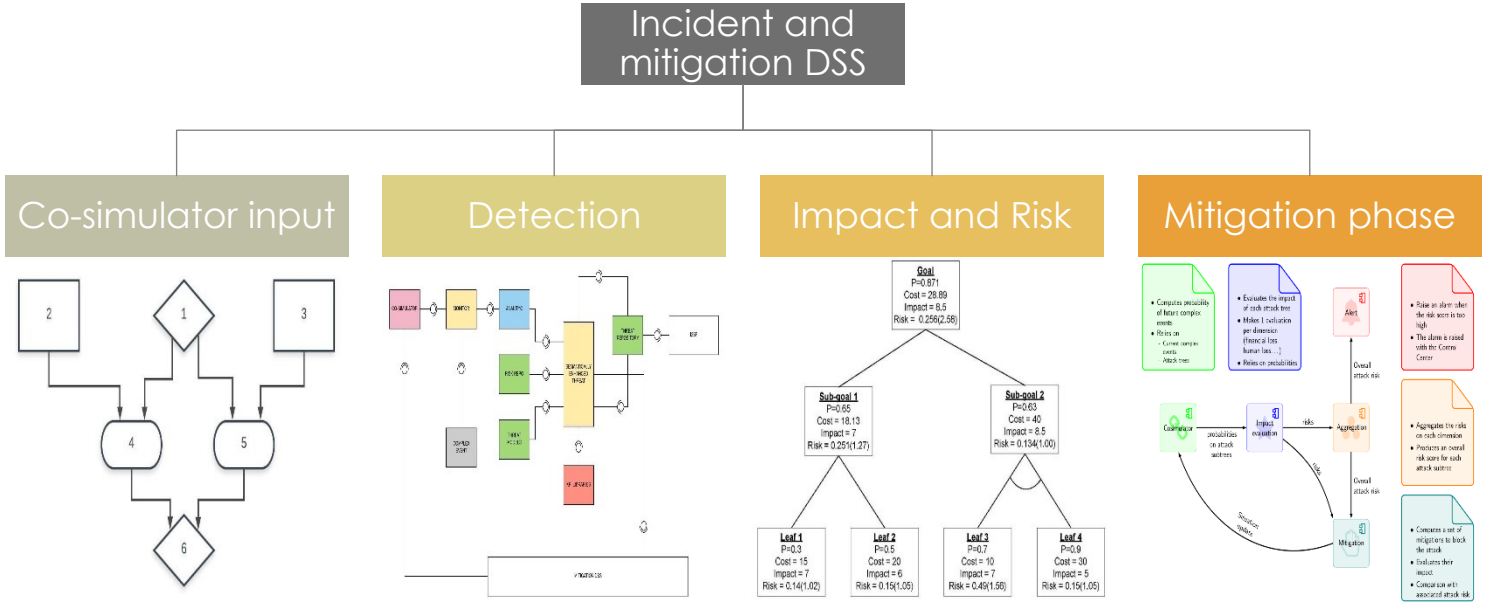
CEI SECURITY AT OPERATIONAL LEVEL

- COUNTERMEASURES TOOLBOX FOR INCIDENT MITIGATION
- DECISION SUPPORT SYSTEMS TO ASSIST CEI SECURITY AUTHORITIES WHEN AUTOMATED MITIGATION IS NOT POSSIBLE
- AVOIDANCE OF CASCADING ATTACKS BY NOTIFICATION & "HUMAN SENSORS"

STATE AWARENESS TO COMPREHENSION

- ATTACK MODELLING BASED ON SEMANTICALLY ENHANCED ATTACK TREES
- EXTENSIVE USE AND COMBINATION OF **BIG DATA ANALYTICS TECHNIQUES AND FRAMEWORKS**
  - **NEAR REAL TIME MEDIA PROCESSING FOR OBJECT EXTRACTION**
  - **DATA MINING ON LOGS**
  - **MACHINE LEARNING FOR INTRUSION DETECTION** (E.G. CLUSTERING & DECISION TREES)
- SECURITY COMPREHENSION AT LOCAL CEI AND PAN-EUROPEAN LEVEL

STATE COMPREHENSION TO MITIGATION

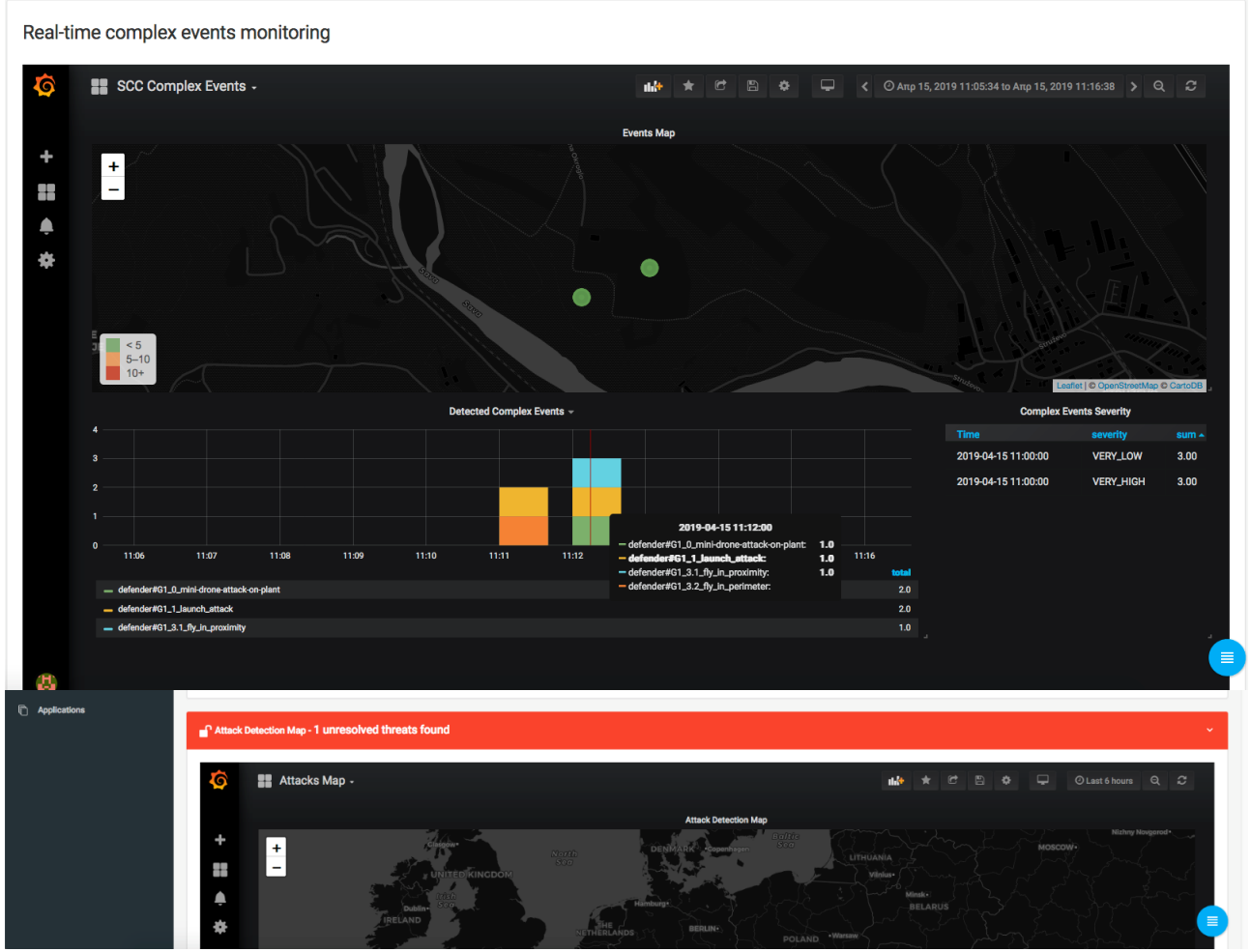


DEFENDER SECURITY CONTROL CENTRE

THE ENTRY POINT TO THE DEFENDER SECURITY PLATFORM, ALLOWING FOR THE GLOBAL OVERVIEW OF THE CEI SECURITY STATUS

FEATURE HIGHLIGHTS:

- REAL-TIME **ATTACKS NOTIFICATIONS**
- CONTEXT-AWARE **APPLICATION OF MITIGATIONS**
- HISTORICAL DATA EXTRACTION
- FULL INTEGRATION WITH THE DEFENDER INCIDENTS AND INFORMATION SHARING PLATFORM



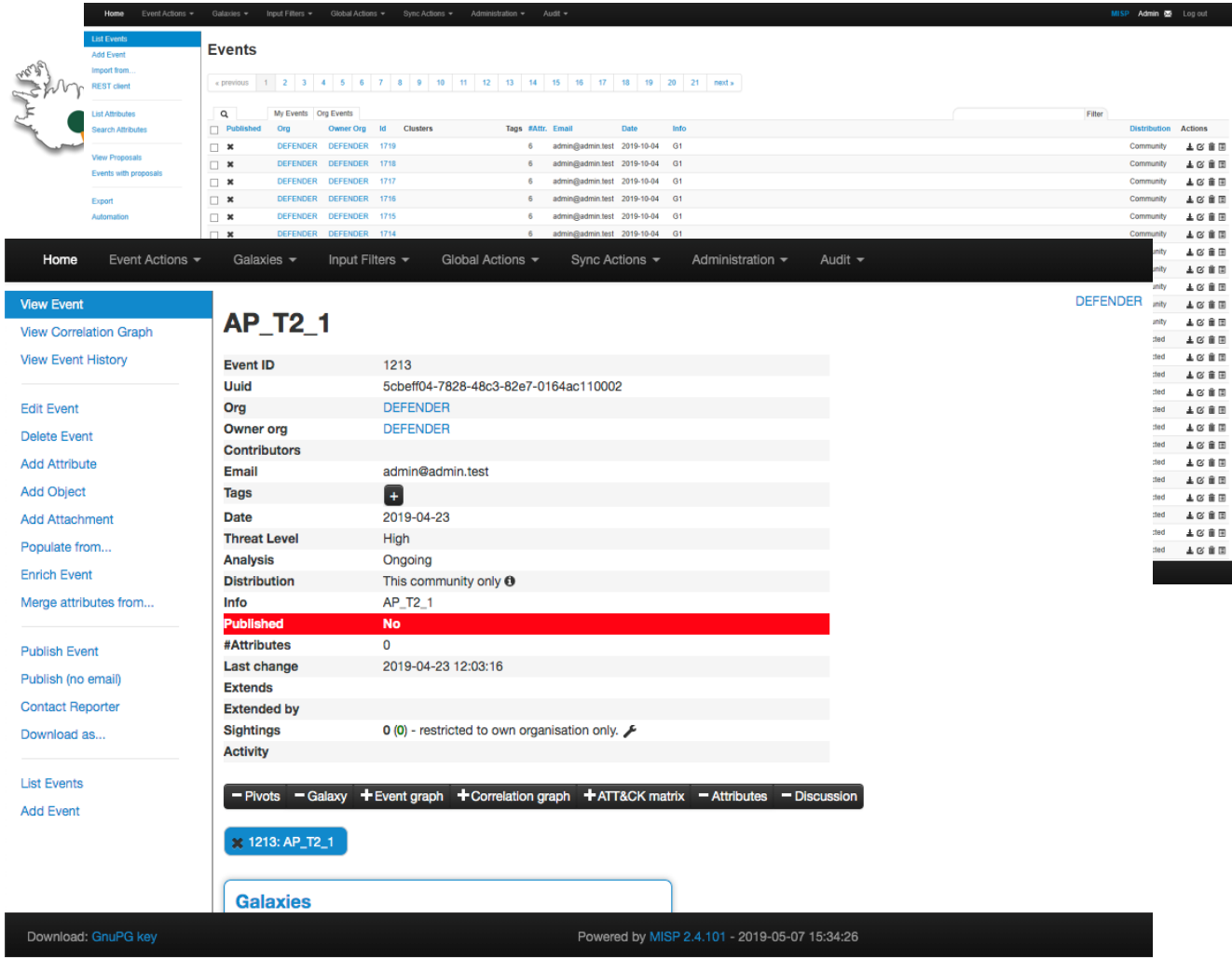
MEDITERRANEAN SECURITY EVENT 2019

DEFENDER I2SP

A PLATFORM (NETWORK) FOR SECURELY SHARING INFORMATION OVER SECURITY INCIDENTS AND VALIDATED ATTACKS AGAINST CEI

FEATURE HIGHLIGHTS:

- **STANDARD INTERFACES** FOR COMMUNICATING INFORMATION (MISP)
- DETECTION OF **ATTACK PATTERNS** AT SPATIOTEMPORAL LEVEL
- DETECTION OF **CASCADING EFFECTS** AND NOTIFICATIONS TOWARDS INTERESTED CEI OWNERS



PEOPLE ACTING AS SECURITY SENSORS

VOLUNTEERS LEAVING IN PROXIMITY OF CEI ACTING AS FIRST RESPONDERS (REPORT VIA SPECIALIZED APPLICATIONS POSSIBLY ACCIDENTS OR SUSPICIOUS INCIDENTS)

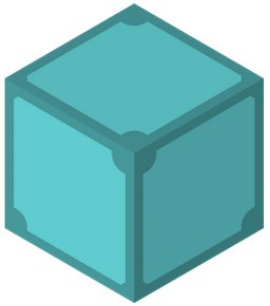
SHORT MESSAGES

PHOTOGRAPHS

VIDEOS

WE NEED TO ENSURE

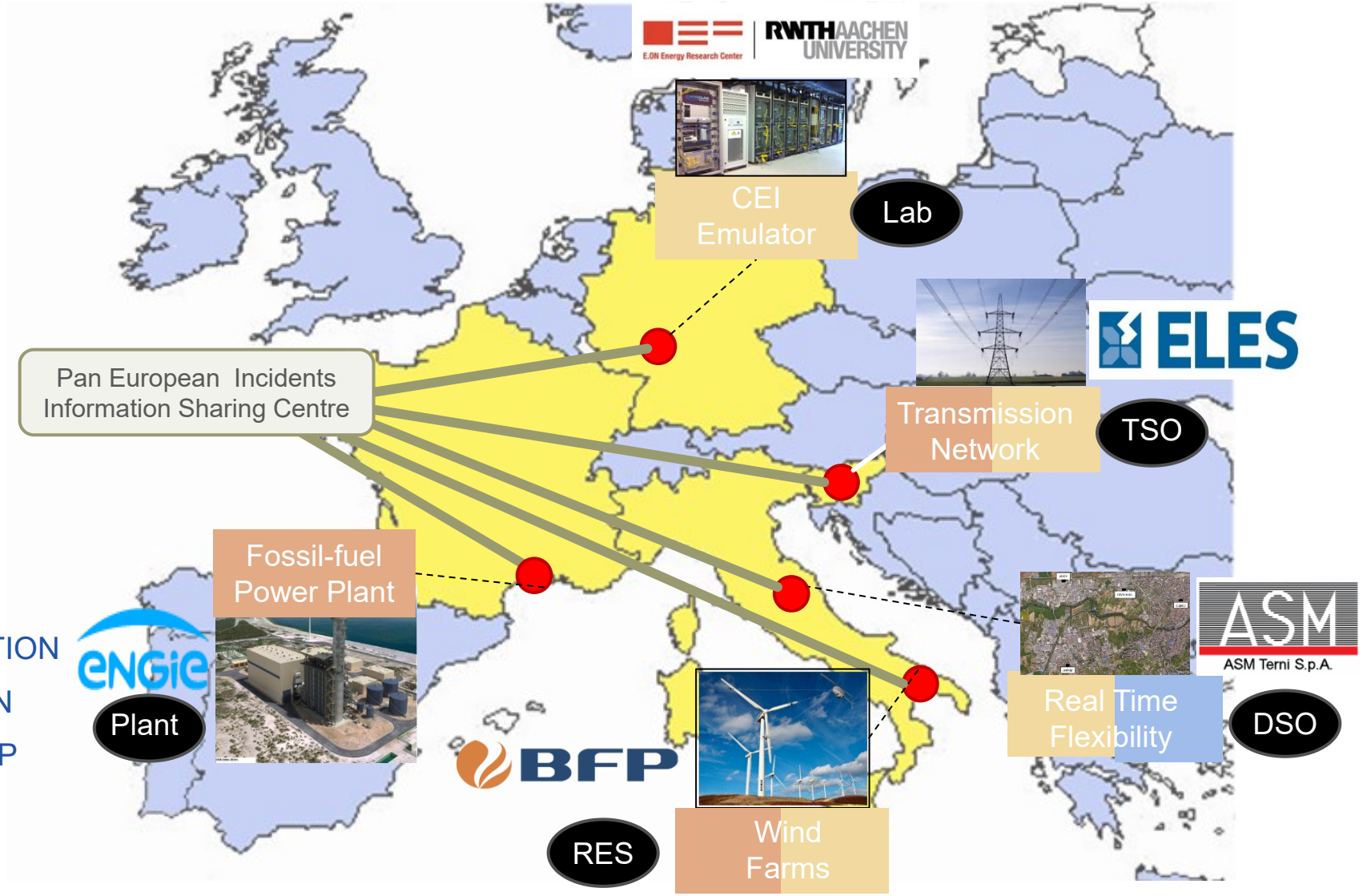
TRUSTED, TRACEABLE, PRIVATE, BI-DIRECTIONAL COMMUNICATIONS



ETHEREUM AS A CONSORTIUM BLOCKCHAIN TO STORE THE IDENTITY

IPFS DISTRIBUTED, ENCRYPTED FILE SYSTEM

END-TO-END ENCRYPTION



- PHYSICAL PROTECTION
- CYBER PROTECTION
- HUMAN IN THE LOOP

ACKNOWLEDGEMENT

THE WORK PRESENTED IN THIS PAPER RECEIVED FUNDING FROM THE EUROPEAN COMMISSION, UNDER THE "CIP-2016-2017-1 TOPIC CIP-01-2016-2017: TOPIC PREVENTION, DETECTION, RESPONSE AND MITIGATION OF THE COMBINATION OF PHYSICAL AND CYBER THREATS TO THE CRITICAL INFRASTRUCTURE OF EUROPE." ENTITLED DEFENDER (DEFENDING THE EUROPEAN ENERGY INFRASTRUCTURES) UNDER GRANT AGREEMENT NUMBER 740898.

MEDITERRANEAN SECURITY EVENT 2019

PLACE YOUR LOGO HERE

Thank you for your attention

DR ARTEMIS VOULKIDIS – ARTEMIS@POWER-OPS.COM